Abstract of Reference 3

SECURITY SYSTEM

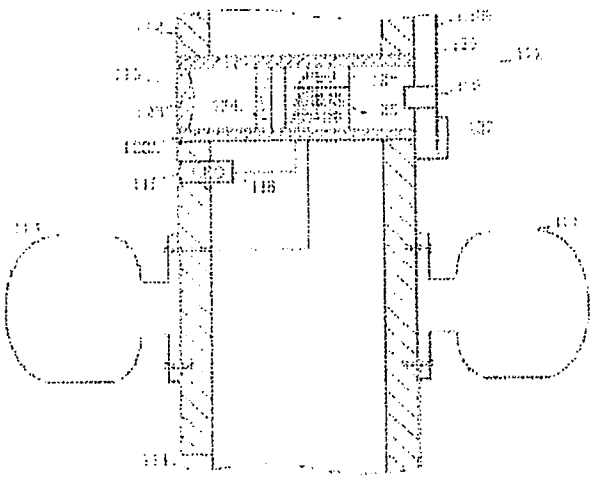
Publication number: JP2003085661 (A)
Publication date: 2003-03-20

Inventor(s): YAMAUCHI UMEO; YAMAGUCHI KANICHI +
Applicant(s): YAMAUCHI JIMUSHO KK; YAMAGUCHI KANICHI +

Classification:
- international: ***B60R25/10; E05B49/00; G03B15/00; G08B13/196; G08B21/00; H04N5/225; H04N7/18;*** *H04N101/00;* **B60R25/10; E05B49/00; G03B15/00; G08B13/194; G08B21/00; H04N5/225; H04N7/18;** (IPC1-7): B60R25/10; E05B49/00; G03B15/00; G08B13/196; G08B21/00; H04N101/00; H04N5/225; H04N7/18
- European:
Application number: JP20010246087 20010814
Priority number(s): JP20010246087 20010814; JP20010180638 20010614; JP20010203062 20010704

Abstract of **JP 2003085661 (A)**

PROBLEM TO BE SOLVED: To provide a security system capable of effectively preventing unauthorized intrusion of a burglar or the like, a robbery or illegal actions. SOLUTION: A hole 116 for illumination is opened on a door 112. An optical lens 123 and a CCD 124 are arranged inside a hole 115 for image pickup, and when there is a visitor 117, it is detected and the image is picked up. Image data processed in an image processing circuit 126 are recorded in a memory 126 sheet by sheet. The image can be viewed on a liquid crystal display 129 and can be taken out from an image data output terminal to the outside as well. The memory 126 can not be detached since it is housed inside the door 112. By photographing the image, the intrusion can be prevented. For the unauthorized intrusion, there is a high possibility of being able to specify the date and time and a face of an intruder or the like by the image. It is also possible to confirm the image or the like and invite the visitor 117 into a prescribed place.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－85661
（P2003－85661A）
(43)公開日　平成15年３月20日(2003.3.20)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０８Ｂ　13/196		Ｃ０８Ｂ　13/196		２Ｅ２５０
Ｂ６０Ｒ　25/10	６２１	Ｂ６０Ｒ　25/10	６２１	５Ｃ０２２
	６２５		６２５	５Ｃ０５４
Ｅ０５Ｂ　49/00		Ｅ０５Ｂ　49/00	Ｋ	５Ｃ０８４
Ｇ０３Ｂ　15/00		Ｃ０３Ｂ　15/00	Ｓ	５Ｃ０８６

審査請求　未請求　請求項の数30　ＯＬ　（全 25 頁）　最終頁に続く

(21)出願番号　特願2001－246087(P2001－246087)

(22)出願日　平成13年８月14日(2001.8.14)

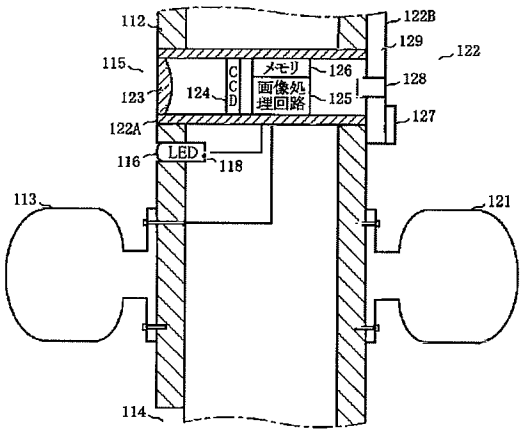
(31)優先権主張番号　特願2001－180638(P2001－180638)
(32)優先日　平成13年６月14日(2001.6.14)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願2001－203062(P2001－203062)
(32)優先日　平成13年７月４日(2001.7.4)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　599172726
有限会社　山内事務所
川崎市麻生区王禅寺1438－288
(71)出願人　598118927
山口　寛一
東京都新宿区西新宿５－17－11
(72)発明者　山内　梅雄
神奈川県川崎市麻生区王禅寺２丁目10番７号
(74)代理人　100083987
弁理士　山内　梅雄

最終頁に続く

(54)【発明の名称】　セキュリティシステム

(57)【要約】
【課題】　泥棒等の無断侵入や盗難あるいは不正行為の発生を有効に防止することのできるセキュリティシステムを得ること。
【解決手段】　ドア１１２には照明用孔１１６が開けられている。撮像用孔１１５の内部には光学レンズ１２３とＣＣＤ１２４が配置されており、来訪者１１７があるとこれが検知されてその画像が撮られる。画像処理回路１２６で処理された画像データはメモリ１２６に１枚ずつ記録される。この画像は液晶ディスプレイ１２９で見ることもできるし画像データ出力端子から外部に取り出すこともできる。メモリ１２６はドア１１２内部に収容されているので、取り外すことができない。画像を撮影することで侵入を防止することができる。無断侵入に対してはその日時および侵入者の顔等を画像で特定できる可能性が高い。画像等を確認して来訪者１１７を所定の場所に招き入れることも可能である。



【特許請求の範囲】
【請求項１】　扉と、
この扉あるいはその近傍に埋め込まれ扉の前の被写体を撮像する撮像手段と、
この撮像手段を作動させるトリガ手段と、
前記扉あるいはその近傍に埋め込まれ、このトリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する撮像データ記憶手段とを具備することを特徴とするセキュリティシステム。
【請求項２】　人の出入りするための扉と、
この扉あるいはその近傍に埋め込まれ扉の前の被写体を撮像する撮像手段と、
この撮像手段を作動させるトリガ手段と、
前記扉あるいはその近傍に埋め込まれ、このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段とを具備することを特徴とするセキュリティシステム。
【請求項３】　ドアの外側部分に突出して取り付けられたドアノブあるいはこのドアノブとドアとの間に配置されたドアノブの台座に穿たれた孔と、
前記ドアの内部側に配置され、この孔を通して外部を撮影する撮像手段と、
この撮像手段を作動させるトリガ手段と、
このトリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する撮像データ記憶手段とを具備することを特徴とするセキュリティシステム。
【請求項４】　ドアの外側部分に突出して取り付けられたドアノブあるいはこのドアノブとドアとの間に配置されたドアノブの台座に穿たれた孔と、
前記ドアの内部側に配置され、この孔を通して外部を撮影する撮像手段と、
この撮像手段を作動させるトリガ手段と、
このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段とを具備することを特徴とするセキュリティシステム。
【請求項５】　交通機関のドアの外側部分に突出して取り付けられたドアの把手あるいはこの把手に取り付けられた付属部品に穿たれた孔と、
前記ドアの内部側に配置され、この孔を通して外部を撮影する撮像手段と、
この撮像手段を作動させるトリガ手段と、
このトリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する撮像データ記憶手段とを具備することを特徴とするセキュリティシステム。
【請求項６】　交通機関のドアの外側部分に突出して取り付けられたドアの把手あるいはこの把手に取り付けられた付属部品に穿たれた孔と、
前記ドアの内部側に配置され、この孔を通して外部を撮影する撮像手段と、
この撮像手段を作動させるトリガ手段と、
このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段とを具備することを特徴とするセキュリティシステム。
【請求項７】　交通機関の所定の部位に穿たれた孔と、
その孔を穿った部分の内部に配置され、この孔を通して外部を撮影する撮像手段と、
この撮像手段を作動させるトリガ手段と、
このトリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する撮像データ記憶手段とを具備することを特徴とするセキュリティシステム。
【請求項８】　交通機関の所定の部位に穿たれた孔と、
その孔を穿った部分の内部に配置され、この孔を通して外部を撮影する撮像手段と、
この撮像手段を作動させるトリガ手段と、
このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段とを具備することを特徴とするセキュリティシステム。
【請求項９】　通路または部屋の壁に埋め込まれ壁の前の被写体を撮像する撮像手段と、
この撮像手段を作動させるトリガ手段と、
前記壁の表面よりも奥側に収容され、このトリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する撮像データ記憶手段とを具備することを特徴とするセキュリティシステム。
【請求項１０】　通路または部屋の壁に埋め込まれ壁の前の被写体を撮像する撮像手段と、
この撮像手段を作動させるトリガ手段と、
前記壁の表面よりも奥側に収容され、このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段とを具備することを特徴とするセキュリティシステム。
【請求項１１】　人の出入りする扉または通路の周辺に配置された防犯以外の所定の用途に使用される容器と、
この容器に穿たれた孔と、
この孔を通して外部を撮影する撮像手段と、
この撮像手段を作動させるトリガ手段と、
このトリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する撮像データ記憶手段とを具備することを特徴とするセキュリティシステム。
【請求項１２】　人の出入りする扉または通路の周辺に配置された防犯以外の所定の用途に使用される容器と、
この容器に穿たれた孔と、
この孔を通して外部を撮影する撮像手段と、
この撮像手段を作動させるトリガ手段と、
このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段とを具備することを特徴とするセキュリティシステ

ム。

【請求項１３】　前記トリガ手段は人等の物体の接近を検出するセンサであることを特徴とする請求項１～請求項１２いずれかに記載のセキュリティシステム。

【請求項１４】　前記トリガ手段は外部の物体の動きを検出して撮像手段を作動させることを特徴とする請求項１～請求項１２いずれかに記載のセキュリティシステム。

【請求項１５】　前記トリガ手段は、予め定めた時間ごとに撮像手段を作動させることを特徴とする請求項１～請求項１２いずれかに記載のセキュリティシステム。

【請求項１６】　前記撮像手段の近傍に外部の音を収集するマイクロフォンが配置されており、収集された音を撮像データと共に処理することを特徴とする請求項１～請求項１２いずれかに記載のセキュリティシステム。

【請求項１７】　前記孔はキーホールに似せた撮像のための孔であることを特徴とする請求項３～請求項８、請求項１１または請求項１２いずれかに記載のセキュリティシステム。

【請求項１８】　撮像の時刻情報が撮像データに組み込まれることを特徴とする請求項１～請求項１２いずれかに記載のセキュリティシステム。

【請求項１９】　前記撮像データ記憶手段は画像を順次１枚ずつ記憶し、予め定められた枚数に到達したときには古い画像から順に上書きして記憶することを特徴とする請求項１、請求項３、請求項５、請求項７、請求項９、請求項１１いずれかに記載のセキュリティシステム。

【請求項２０】　前記所定の受信先は予め定めた携帯端末等の通信端末であることを特徴とする請求項２、請求項４、請求項６、請求項８、請求項１０、請求項１２いずれかに記載のセキュリティシステム。

【請求項２１】　前記所定の受信先は駐輪場あるいは駐車場等に設けられた集中管理用の通信端末であり、それぞれの発信元ごとにデータが管理されることを特徴とする請求項２、請求項４、請求項６、請求項８、請求項１０、請求項１２いずれかに記載のセキュリティシステム。

【請求項２２】　人の出入りするための扉と、
この扉あるいはその近傍に埋め込まれ扉の前の被写体を撮像する撮像手段と、
この撮像手段を作動させるトリガ手段と、
前記扉あるいはその近傍に埋め込まれ、このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段と、
この撮像データ発信手段の発信に基づく前記受信先との通信中に受信先から開錠を指示する信号が送られてきたとき前記扉を開錠する開錠手段とを具備することを特徴とするセキュリティシステム。

【請求項２３】　人の出入りするための扉と、
この扉あるいはその近傍に埋め込まれ扉の前の被写体を撮像する撮像手段と、
この撮像手段を作動させるトリガ手段と、
前記扉あるいはその近傍に埋め込まれ、このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段と、
この撮像データ発信手段の受信先に撮像データを発信できないとき、予め定めた宛先にこれを転送する転送手段と、
この撮像データ発信手段の発信に基づく前記宛先との通信中にその宛先から開錠を指示する信号が送られてきたとき前記扉を開錠する開錠手段とを具備することを特徴とするセキュリティシステム。

【請求項２４】　前記孔から前記撮像手段が撮像する障害となる明るさの変化を検出する障害検出手段と、この障害検出手段の検出が行われたとき警報音を出力する警報音出力手段を具備することを特徴とする請求項３～８いずれかに記載のセキュリティシステム。

【請求項２５】　前記孔から前記撮像手段が撮像する障害となる明るさの変化を検出する障害検出手段と、この障害検出手段の検出が行われたとき警報を示すデータを所定の宛先に送出する警報データ送出手段を具備することを特徴とする請求項３～８いずれかに記載のセキュリティシステム。

【請求項２６】　前記孔は複数配置されており、前記トリガ手段は、障害検出手段が１つの孔の障害を検出したとき他の孔の内部に配置された前記撮像手段を作動させることを特徴とする請求項２４または請求項２５記載のセキュリティシステム。

【請求項２７】　交通機関の走行のための動力源が始動されたときこれを検出する動力源始動検出手段と、
この動力源始動検出手段が動力源の始動を検出したときその周囲にその交通機関の所有者の所持する特定通信端末が存在するか否かを通信によって判別する特定通信端末有無判別手段と、
この特定通信端末有無判別手段がその特定通信端末が存在しないと判別したときその特定通信端末に対して前記交通機関の動力源が始動されたことを無線で通知する通知手段とを具備することを特徴とするセキュリティシステム。

【請求項２８】　交通機関の走行のための動力源を作動させるキーを挿入するキー挿入口と、
このキー挿入口にキーが挿入され前記動力源が始動されたときこれを検出する動力源始動検出手段と、
この動力源始動検出手段が動力源の始動を検出したときその周囲にその交通機関のキー所有者の所持する特定通信端末が存在するか否かを通信によって判別する特定通信端末有無判別手段と、
この特定通信端末有無判別手段がその特定通信端末が存在しないと判別したときその特定通信端末に対して前記

交通機関の動力源が始動されたことを無線で通知する通知手段とを具備することを特徴とするセキュリティシステム。

【請求項２９】　前記交通機関の運転席あるいはその近傍を撮像する撮像手段を備え、前記通知手段はこの撮像した画像を添付して前記特定通信端末にこれを送信することを特徴とする請求項２７または請求項２８記載のセキュリティシステム。

【請求項３０】　前記通知手段の通知に基づいて前記特定通信端末から前記交通機関の走行停止あるいはドアのロックを示す信号が送信されてきたときこれに応じてその交通機関の走行停止あるいはドアのロックを行う交通機関側制御手段を具備することを特徴とする請求項２７または請求項２８記載のセキュリティシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は盗難、無断侵入を防止したり、所定の場所を出入りする者をチェックあるいは管理するためのセキュリティシステムに係わり、たとえば自動車、バイク、船舶等の交通機関、家屋、金庫、エレベータ、洗面所の入り口、飛行機の搭乗口等の各物あるいは場所で使用することのできるセキュリティシステムに関する。

【０００２】

【従来の技術】家屋や車に対する無断侵入や金庫等の保管容器内の物品の盗難を防止する等のために鍵が広く使用されている。また、防犯用のテレビカメラも使用されている。

【０００３】

【発明が解決しようとする課題】ところが、通常の鍵は熟練した泥棒の多くが簡単に開けることができる。このため、より複雑な構造をした鍵が考案されているが、時間をかければそのほとんどが開けられてしまう。したがって、現状では玄関ドアに複数の鍵を付けて、泥棒が開けるまでの時間を稼ぐことで泥棒に侵入を敬遠させるといった手法が勧められている。しかしながら、泥棒が一度ドアを開けて侵入してしまえば、その者の足跡は掴みにくいのが通常であり、事件は未解決に終わることも多い。

【０００４】また、防犯用のテレビカメラはその位置および撮影範囲が外部から特定されるので、その死角を利用して犯罪が行われることがある。また、テレビカメラ自体を事前に撮影不能にすることも場合によって可能である。更にテレビカメラの設置にはある程度の場所が必要であって、小型の自動車や金庫等に配置することができない。また、設備の購入および維持のためのコストがかなり高いという問題もある。

【０００５】以上、泥棒を中心に説明したが、テレビカメラは人の管理にも使用されているものの、同様の問題がある。

【０００６】そこで本発明の目的は、泥棒等の無断侵入や盗難あるいは不正行為の発生を有効に防止することのできるセキュリティシステムを提供することにある。

【０００７】

【課題を解決するための手段】請求項１記載の発明では、（イ）扉と、（ロ）この扉あるいはその近傍に埋め込まれ扉の前の被写体を撮像する撮像手段と、（ハ）この撮像手段を作動させるトリガ手段と、（ニ）扉あるいはその近傍に埋め込まれ、このトリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する撮像データ記憶手段とをセキュリティシステムに具備させる。

【０００８】すなわち請求項１記載の発明では、撮像手段が扉あるいはその近傍に埋め込まれており、扉の前の被写体を撮像するようになっている。撮像データ記憶手段は、扉あるいはその近傍に埋め込まれており、トリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶するようになっている。撮像手段がデジタルカメラの普及によって小型化かつ高性能化したので、たとえばその構成部品を扉あるいはその近傍に埋め込むことが可能になる。撮像データ記憶手段も、扉あるいはその近傍に埋め込まれるので、自分が撮影されたことに気づいた侵入者等は撮影された画像を消去したり撮像データ記憶手段自体を取り出すことが困難であり、早急に現場を立ち去ることになるので、無断侵入や盗難あるいは不正行為の発生を有効に防止することができる。撮像データとして動画を得ることも可能であるが、特に静止画を得る場合には、僅かのメモリ容量で多くの静止画を得ることができる。また銀塩写真と比べてランニングコストをわずかに抑えることができ、また事件が起きたときには画像データを有効な資料とすることができる。

【０００９】請求項２記載の発明では、（イ）人の出入りするための扉と、（ロ）この扉あるいはその近傍に埋め込まれ扉の前の被写体を撮像する撮像手段と、（ハ）この撮像手段を作動させるトリガ手段と、（ニ）扉あるいはその近傍に埋め込まれ、このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段とをセキュリティシステムに具備させる。

【００１０】すなわち請求項２記載の発明では、撮像手段が扉あるいはその近傍に埋め込まれており、扉の前の被写体を撮像するようになっている。撮像データ発信手段は、扉あるいはその近傍に埋め込まれており、トリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信するようになっている。撮像手段がデジタルカメラの普及によって小型化かつ高性能化したので、たとえばその構成部品を扉あるいはその近傍に埋め込むことが可能になる。撮像データ発信手段も扉あるいはその近傍に埋め込まれているので、発信を安全に行うことができる。しかも本発明の場合には画像自体は

所定の受信先に送られてしまうので、仮に撮像手段や撮像データ発信手段が持ち去られたとしても、画像の記録は残ることになり、結局、無断侵入や盗難あるいは不正行為の発生を有効に防止することができる。撮像データとして動画を得ることも可能であるが、特に静止画を得る場合には、多くの画像を短時間に送信することができる。

【００１１】請求項３記載の発明では、（イ）ドアの外側部分に突出して取り付けられたドアノブあるいはこのドアノブとドアとの間に配置されたドアノブの台座に穿たれた孔と、（ロ）ドアの内部側に配置され、この孔を通して外部を撮影する撮像手段と、（ハ）この撮像手段を作動させるトリガ手段と、（ニ）このトリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する撮像データ記憶手段とをセキュリティシステムに具備させる。

【００１２】すなわち請求項３記載の発明では、ドアの外側部分に突出して取り付けられたドアノブあるいはこのドアノブとドアとの間に配置されたドアノブの台座に孔を穿っている。撮像手段はドアの内部側に配置され、この孔を通して外部を撮影するようになっている。撮像データ記憶手段は、トリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する。このように小型化された撮像のための装置をドアノブあるいはこのドアノブとドアとの間に配置されたドアノブの台座の孔から撮影することにしたので、ドア自体を加工する必要がない。ドアノブに本発明を適用することで、無断侵入や盗難あるいは不正行為の発生を有効に防止することができる。また、台座の表面に凹凸を付けるといったようにデザインを工夫すれば、孔の存在を判りにくくすることができる。

【００１３】請求項４記載の発明では、（イ）ドアの外側部分に突出して取り付けられたドアノブあるいはこのドアノブとドアとの間に配置されたドアノブの台座に穿たれた孔と、（ロ）ドアの内部側に配置され、この孔を通して外部を撮影する撮像手段と、（ハ）この撮像手段を作動させるトリガ手段と、（ニ）このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段とをセキュリティシステムに具備させる。

【００１４】すなわち請求項４記載の発明では、ドアの外側部分に突出して取り付けられたドアノブあるいはこのドアノブとドアとの間に配置されたドアノブの台座に孔を穿っている。撮像手段はドアの内部側に配置され、この孔を通して外部を撮影するようになっている。撮像データ発信手段は、トリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する。したがって、事故の発生や友人等の来訪を迅速に知ることができる。更に撮像データを発信することにしたので、ドアノブ側に大量のメモリが不要であり、大量の静止画だけでなく、動画を撮る時間の制限も緩和される。また、台座の表面に凹凸を付けるといったようにデザインを工夫すれば、孔の存在を判りにくくすることができる。

【００１５】請求項５記載の発明では、（イ）交通機関のドアの外側部分に突出して取り付けられたドアの把手あるいはこの把手に取り付けられた付属部品に穿たれた孔と、（ロ）ドアの内部側に配置され、この孔を通して外部を撮影する撮像手段と、（ハ）この撮像手段を作動させるトリガ手段と、（ニ）このトリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する撮像データ記憶手段とをセキュリティシステムに具備させる。

【００１６】すなわち請求項５記載の発明では、自動車、船等の交通機関のドアの外側部分に突出して取り付けられたドアの把手あるいはこの把手に取り付けられた付属部品に孔を穿っている。撮像手段はドアの内部側に配置され、この孔を通して外部を撮影するようになっている。撮像データ記憶手段は、トリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する。このように小型化された撮像のための装置をドアの把手あるいはこの把手に取り付けられた付属部品の孔から撮影することにしたので、ドア自体を加工する必要がない。ドアの把手あるいはこの把手に取り付けられた付属部品を本発明のものとすることで、無断侵入や盗難あるいは不正行為の発生を有効に防止することができる。

【００１７】請求項６記載の発明では、（イ）交通機関のドアの外側部分に突出して取り付けられたドアの把手あるいはこの把手に取り付けられた付属部品に穿たれた孔と、（ロ）ドアの内部側に配置され、この孔を通して外部を撮影する撮像手段と、（ハ）この撮像手段を作動させるトリガ手段と、（ニ）このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段とをセキュリティシステムに具備させる。

【００１８】すなわち請求項６記載の発明では、自動車、船等の交通機関のドアの外側部分に突出して取り付けられたドアの把手あるいはこの把手に取り付けられた付属部品に孔を穿っている。撮像手段はドアの内部側に配置され、この孔を通して外部を撮影するようになっている。撮像データ発信手段は、トリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する。したがって、その交通機関自体が盗難にあった場合も画像データ自体は安全な箇所に保持されることになり、盗難の犯人の特定が容易になる。また、結果的には盗難あるいは不正行為の発生を有効に防止することができる。

【００１９】請求項７記載の発明では、（イ）交通機関の所定の部位に穿たれた孔と、（ロ）その孔を穿った部分の内部に配置され、この孔を通して外部を撮影する撮

像手段と、（ハ）この撮像手段を作動させるトリガ手段と、（ニ）このトリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する撮像データ記憶手段とをセキュリティシステムに具備させる。

【００２０】すなわち請求項７記載の発明では、請求項５および請求項６と異なり、ドアの把手あるいはこの把手に取り付けられた付属部品以外の場所でも孔を開けることができれば、同様に本発明を適用可能であることを示している。交通機関の外側に予め荷物を止めるための部品やバックミラー等の部品が配置されている場合には、これらの部品の内部に撮像手段等を収容すればよい。これらの部品を必要に応じて交換することで、本発明による盗難防止等の利益を得ることができる。

【００２１】請求項８記載の発明では、（イ）交通機関の所定の部位に穿たれた孔と、（ロ）その孔を穿った部分の内部に配置され、この孔を通して外部を撮影する撮像手段と、（ハ）この撮像手段を作動させるトリガ手段と、（ニ）このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段とをセキュリティシステムに具備させる。

【００２２】すなわち請求項８記載の発明では、請求項５および請求項６と異なり、ドアの把手あるいはこの把手に取り付けられた付属部品以外の場所でも孔を開けることができれば、同様に本発明を適用可能であることを示している。交通機関の外側に予め荷物を止めるための部品やバックミラー等の部品が配置されている場合には、これらの部品の内部に撮像手段等を収容すればよい。これらの部品を必要に応じて交換することで、本発明による盗難防止等の利益を得ることができる。しかも本発明では撮像データ発信手段を配置しているので、画像データ自体は安全な場所に送信され、かつ画像データを早期に取得できることになる。

【００２３】請求項９記載の発明では、（イ）通路または部屋の壁に埋め込まれ壁の前の被写体を撮像する撮像手段と、（ロ）この撮像手段を作動させるトリガ手段と、（ハ）壁の表面よりも奥側に収容され、このトリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する撮像データ記憶手段とをセキュリティシステムに具備させる。

【００２４】すなわち請求項９記載の発明では、撮像手段が通路または部屋の壁に埋め込まれ壁の前の被写体を撮像することができるようになっている。撮像データ記憶手段は、壁の表面よりも奥側に収容され、このトリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶するようになっている。壁の表面よりも奥側とは、必ずしも壁の内部とは限らず、たとえばその壁の向こう側の部屋の内部や天井部分であってもよい。要は第三者が撮像データ記憶手段に対してアクセスしにくい場所をいう。本発明でも、撮影された者はなす術がないので、結局、無断侵入や盗難あるいは不正行為の発生を有効に防止することができることになる。

【００２５】請求項１０記載の発明では、（イ）通路または部屋の壁に埋め込まれ壁の前の被写体を撮像する撮像手段と、（ロ）この撮像手段を作動させるトリガ手段と、（ハ）壁の表面よりも奥側に収容され、このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段とをセキュリティシステムに具備させる。

【００２６】すなわち請求項１０記載の発明では、撮像手段が通路または部屋の壁に埋め込まれ壁の前の被写体を撮像することができるようになっている。撮像データ発信手段は、壁の表面よりも奥側に収容され、このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信するようになっている。壁の表面よりも奥側とは、必ずしも壁の内部とは限らず、たとえばその壁の向こう側の部屋の内部や天井部分であってもよい。要は第三者が撮像データ記憶手段に対してアクセスしにくい場所をいう。本発明でも、撮影された者はなす術がないので、結局、無断侵入や盗難あるいは不正行為の発生を有効に防止することができることになる。しかも本発明では撮像データ発信手段を配置しているので、画像データ自体は安全な場所に送信され、かつ画像データを早期に取得できることになる。

【００２７】請求項１１記載の発明では、（イ）人の出入りする扉または通路の周辺に配置された防犯以外の所定の用途に使用される容器と、（ロ）この容器に穿たれた孔と、（ハ）この孔を通して外部を撮影する撮像手段と、（ニ）この撮像手段を作動させるトリガ手段と、（ホ）このトリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する撮像データ記憶手段とをセキュリティシステムに具備させる。

【００２８】すなわち請求項１１記載の発明では、郵便受けやドアホン等のように人の出入りする扉または通路の周辺に配置された防犯以外の所定の用途に使用される容器に孔を穿ち、撮像手段でこの孔を通して外部を撮影するようにしている。撮像データ記憶手段は、トリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶するようになっている。借家住まいのように扉または通路自体の改造が難しい場合には、このような容器を適所に取り付けることで、泥棒等の無断侵入や盗難あるいは不正行為の発生を有効に防止することができることになる。

【００２９】請求項１２記載の発明では、（イ）人の出入りする扉または通路の周辺に配置された防犯以外の所定の用途に使用される容器と、（ロ）この容器に穿たれた孔と、（ハ）この孔を通して外部を撮影する撮像手段と、（ニ）この撮像手段を作動させるトリガ手段と、（ホ）このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段とをセキュリティシステムに具備させる。

【００３０】すなわち請求項１２記載の発明では、郵便受けやドアホン等のように人の出入りする扉または通路の周辺に配置された防犯以外の所定の用途に使用される容器に孔を穿ち、撮像手段でこの孔を通して外部を撮影するようにしている。撮像データ発信手段は、トリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信するようになっている。したがって、その容器自体を破壊されたり持ち去られるような場合でも、その行為を行った者の画像を取得することができ、結果的にそのような行為自体も防止することができる。

【００３１】請求項１３記載の発明では、請求項１～請求項１２いずれかに記載のセキュリティシステムで、トリガ手段は人等の物体の接近を検出するセンサであることを特徴としている。

【００３２】すなわち請求項１３記載の発明では、画像の撮影を開始するトリガ手段は人等の物体の接近を検出するセンサであることを特徴としている。撮影は静止画であれば１枚または所定枚数を間隔を置いて行う。センサが検知している期間に渡って所定間隔で静止画を撮り続けるようなものであってもよい。動画であればその期間あるいはタイマによって設定した時間だけ画像を撮り続けることになる。

【００３３】請求項１４記載の発明では、請求項１～請求項１２いずれかに記載のセキュリティシステムで、トリガ手段は外部の物体の動きを検出して撮像手段を作動させることを特徴としている。

【００３４】すなわち請求項１４記載の発明では、画像の撮影を開始するトリガ手段は外部の物体の動きを検出して撮像手段を作動させることを特徴としている。撮影は静止画であれば１枚または所定枚数を間隔を置いて行う。センサが検知している期間に渡って所定間隔で静止画を撮り続けるようなものであってもよい。動画であればその期間あるいはタイマによって設定した時間だけ画像を撮り続けることになる。動きを検出するので、人の接近等を効果的に検出できる。

【００３５】請求項１５記載の発明では、請求項１～請求項１２いずれかに記載のセキュリティシステムで、トリガ手段は、予め定めた時間ごとに撮像手段を作動させることを特徴としている。

【００３６】すなわち請求項１５記載の発明では、画像の撮影を開始するトリガ手段は、たとえば１分置きというように予め定めた時間ごとに撮像手段を作動させる。静止画であれば画像データの１枚あたりの量はそれほど多くないので、半導体のメモリであっても数日分の画像を簡単に記憶させることができる。また、画像データを送信する場合には発信側にメモリ容量の制限がないので、時間間隔を狭めても問題が生じることは少ない。本発明では、トリガ用に特別のセンサが不要であるので、確実に無断侵入や盗難あるいは不正行為の事実を記録することができる。

【００３７】請求項１６記載の発明では、請求項１～請求項１２いずれかに記載のセキュリティシステムで、撮像手段の近傍に外部の音を収集するマイクロフォンが配置されており、収集された音を撮像データと共に処理することを特徴としている。

【００３８】すなわち請求項１６記載の発明では、画像データと共に音のデータも収集することを示している。音の収集だけでなく発声も行えるようにすれば、自宅を留守にしているような場合でも、ドアホンを使用している感覚で携帯電話機等を使用して訪問者等と会話が可能になる。

【００３９】請求項１７記載の発明では、請求項３～請求項８、請求項１１または請求項１２いずれかに記載のセキュリティシステムで、孔はキーホールに似せた撮像のための孔であることを特徴としている。

【００４０】すなわち請求項１７記載の発明では、撮像のための孔をキーホールに似せたものにすることでカムフラージュして、本人が気付かないうちに撮影を可能にしている。孔を開けた周囲のデザインを工夫して撮像手段が存在することを気づかせないようにすることも場合により有効である。

【００４１】請求項１８記載の発明では、請求項１～請求項１２いずれかに記載のセキュリティシステムで、撮像の時刻情報が撮像データに組み込まれることを特徴としている。

【００４２】すなわち請求項１８記載の発明では、撮像の時刻情報が撮像データに組み込まれると、泥棒等の無断侵入や盗難あるいは不正行為の起きた日時を推測できる可能性が高くなる。また、子供が学校から帰ってきた時間等も簡単に知ることができる。

【００４３】請求項１９記載の発明では、請求項１、請求項３、請求項５、請求項７、請求項９、請求項１１いずれかに記載のセキュリティシステムで、撮像データ記憶手段は画像を順次１枚ずつ記憶し、予め定められた枚数に到達したときには古い画像から順に上書きして記憶することを特徴としている。

【００４４】すなわち請求項１９記載の発明では、記憶手段に静止画の画像データを１枚ずつ記憶する場合には、ある程度のメモリ容量に対して古い画像から順に上書きして記憶することで、メモリ不足を解消することができ、特別の事件が起きた時点で画像データを確実に再現することができる。

【００４５】請求項２０記載の発明では、請求項２、請求項４、請求項６、請求項８、請求項１０、請求項１２いずれかに記載のセキュリティシステムで、前記した所定の受信先は予め定めた携帯端末等の通信端末であることを特徴としている。

【００４６】すなわち請求項２０記載の発明では、携帯端末を受信先とすることで迅速な対応が可能になる。ま

た撮像側に音声の入出力装置を備えることで、訪問者との会話も可能になる。

【００４７】請求項２１記載の発明では、請求項２、請求項４、請求項６、請求項８、請求項１０、請求項１２いずれかに記載のセキュリティシステムで、前記した所定の受信先は駐輪場あるいは駐車場等に設けられた集中管理用の通信端末であり、それぞれの発信元ごとにデータが管理されることを特徴としている。

【００４８】すなわち請求項２１記載の発明では、所定の受信先が駐輪場あるいは駐車場等に設けられた集中管理用の通信端末であり、それぞれの発信元ごとにデータが管理されれば、安価に盗難やいたずらの防止が可能になる。

【００４９】請求項２２記載の発明では、（イ）人の出入りするための扉と、（ロ）この扉あるいはその近傍に埋め込まれ扉の前の被写体を撮像する撮像手段と、（ハ）この撮像手段を作動させるトリガ手段と、（ニ）扉あるいはその近傍に埋め込まれ、このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段と、（ホ）この撮像データ発信手段の発信に基づく受信先との通信中に受信先から開錠を指示する信号が送られてきたとき扉を開錠する開錠手段とをセキュリティシステムに具備させる。

【００５０】すなわち請求項２２記載の発明では、撮像データを扉の配置されている側から所定の受信先に発信し、この通信中に受信先から開錠を指示する信号が送られてきたとき扉を開錠するので、扉の前の被写体を撮像データで確認したり音声による確認が可能であり、開錠の適否を的確に判別することができる。しかも、第三者の発呼によって開錠するのと異なるので、セキュリティを高度に保持することができる。

【００５１】請求項２３記載の発明では、（イ）人の出入りするための扉と、（ロ）この扉あるいはその近傍に埋め込まれ扉の前の被写体を撮像する撮像手段と、（ハ）この撮像手段を作動させるトリガ手段と、（ニ）扉あるいはその近傍に埋め込まれ、このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段と、（ホ）この撮像データ発信手段の受信先に撮像データを発信できないとき、予め定めた宛先にこれを転送する転送手段と、（ヘ）この撮像データ発信手段の発信に基づく宛先との通信中にその宛先から開錠を指示する信号が送られてきたとき扉を開錠する開錠手段とをセキュリティシステムに具備させる。

【００５２】すなわち請求項２３記載の発明では、撮像データ発信手段の受信先に撮像データを発信できないとき、予め定めた宛先にこれを転送し、その転送先がこれによる通信を行っている場合に限って遠隔操作による開錠を可能にしたので、本来の受信先の都合によって扉を開けるまでの待ち時間が長くなったり不可能となるといった事態が発生しない。また、本発明の場合にも扉の前の被写体を撮像データで確認したり音声による確認が可能であり、開錠の適否を的確に判別することができる。しかも、第三者の発呼によって開錠するのと異なるので、セキュリティを高度に保持することができる。

【００５３】請求項２４記載の発明では、請求項３～８いずれかに記載のセキュリティシステムで、孔から撮像手段が撮像する障害となる明るさの変化を検出する障害検出手段と、この障害検出手段の検出が行われたとき警報音を出力する警報音出力手段を具備することを特徴としている。

【００５４】すなわち請求項２４記載の発明では、撮影を行うための孔の工作を行って撮影を妨害するような場合に警報音を出力することにしたので、このような妨害を効率的に排除することができる。

【００５５】請求項２５記載の発明では、請求項３～８いずれかに記載のセキュリティシステムで、孔から撮像手段が撮像する障害となる明るさの変化を検出する障害検出手段と、この障害検出手段の検出が行われたとき警報を示すデータを所定の宛先に送出する警報データ送出手段を具備することを特徴としている。

【００５６】すなわち請求項２５記載の発明では、撮影を行うための孔の工作を行って撮影を妨害するような場合に警報を示すデータを所定の宛先に送出する警報データ送出手段を具備させたので、家屋の侵入や自動車等の盗難等が行われる際にこれを所有者等の所定の者に迅速に知らせることができるようになる。

【００５７】請求項２６記載の発明では、請求項３～８いずれかに記載のセキュリティシステムで、孔は複数配置されており、トリガ手段は、障害検出手段が１つの孔の障害を検出したとき他の孔の内部に配置された撮像手段を作動させることを特徴としている。

【００５８】すなわち請求項２６記載の発明では、撮影を行うための孔を複数配置し、障害検出手段が１つの孔の障害を検出したとき他の孔の内部に配置された撮像手段を作動させることにしたので、撮影の妨害を行う者が１つの孔を塞ぐ等の行為を行っても、他の孔を通じて画像を取得することができ、セキュリティを向上させることができる。

【００５９】請求項２７記載の発明では、（イ）交通機関の走行のための動力源が始動されたときこれを検出する動力源始動検出手段と、（ロ）この動力源始動検出手段が動力源の始動を検出したときその周囲にその交通機関の所有者の所持する特定通信端末が存在するか否かを通信によって判別する特定通信端末有無判別手段と、（ハ）この特定通信端末有無判別手段がその特定通信端末が存在しないと判別したときその特定通信端末に対して前記した交通機関の動力源が始動されたことを無線で通知する通知手段とをセキュリティシステムに具備させ

る。

【００６０】すなわち請求項２７記載の発明では、交通機関を走行させる者の多くが自己の通信のための携帯電話機等の通信端末を所持している事実に鑑みて、動力源始動検出手段が何らかの操作で動力源の始動を検出したときその周囲にその者の通信端末（特定通信端末）が存在していないときにはその特定通信端末に無線で通知することで、第三者による交通機関の無断走行等に対処することにしたものである。なお、その通知後の交通機関については、走行を停止させたり、所定の速度以上の速度が出ないようにすることも特定通信端末からの制御で可能である。運転席等のドアをロックして運転を試みた者が車外に逃げ出すまでの時間を稼ぐことも可能である。もちろん、一度このような措置を行った者は、その後、運転できない状態を解除したり、ドアのロックを解除することができる。このような操作は、特定通信端末に割り振られたキースイッチを操作することによって簡単に実現することがきる

【００６１】請求項２８記載の発明では、（イ）交通機関の走行のための動力源を作動させるキーを挿入するキー挿入口と、（ロ）このキー挿入口にキーが挿入され前記した動力源が始動されたときこれを検出する動力源始動検出手段と、（ハ）この動力源始動検出手段が動力源の始動を検出したときその周囲にその交通機関のキー所有者の所持する特定通信端末が存在するか否かを通信によって判別する特定通信端末有無判別手段と、（ニ）この特定通信端末有無判別手段がその特定通信端末が存在しないと判別したときその特定通信端末に対してその交通機関の動力源が始動されたことを無線で通知する通知手段とをセキュリティシステムに具備させる。

【００６２】すなわち請求項２８記載の発明では、交通機関を走行させるためのキーを所持する者の多くが自己の通信のための携帯電話機等の通信端末を所持している事実に鑑みて、動力源始動検出手段がキーの操作による動力源の始動を検出したときその周囲にその者の通信端末（特定通信端末）が存在していないときにはその特定通信端末に無線で通知することで、第三者によるキーを用いた交通機関の無断走行等に対処することにしたものである。なお、その通知後の交通機関については、走行を停止させたり、所定の速度以上の速度が出ないようにすることも特定通信端末からの制御で可能である。

【００６３】請求項２９記載の発明では、請求項２７または請求項２８記載のセキュリティシステムで、交通機関の運転席あるいはその近傍を撮像する撮像手段を備え、通知手段はこの撮像した画像を添付して特定通信端末にこれを送信することを特徴としている。

【００６４】すなわち請求項２９記載の発明では、たとえばキー挿入口の近傍等の第三者が気づきにくい位置等に撮像手段を配置しておけば、これらの者が不正に運転を試みた場合にその者の画像を特定通信端末に送信することが可能になる。また、家族がその交通機関を運転しようとしていたような場合には、画像を見ることによって第三者が不正に操作しているものでないことを簡単に確認することができる。

【００６５】請求項３０記載の発明では、請求項２７または請求項２８記載のセキュリティシステムで、通知手段の通知に基づいて前記した特定通信端末から交通機関の走行停止あるいはドアのロックを示す信号が送信されてきたときこれに応じてその交通機関の走行停止あるいはドアのロックを行う交通機関側制御手段を具備している。

【００６６】すなわち請求項３０記載の発明では、交通機関が高速あるいは長時間運行することで、行方をくらましたり不正に運転を行った者が運転席から逃げるような事態の発生も防止している。特定通信端末側では必要に応じてこのような措置を解除する電波を送信することもできる。

【００６７】

【発明の実施の形態】

【００６８】

【実施例】以下実施例につき本発明を詳細に説明する。

【００６９】第１の実施例

【００７０】図１は本発明の第１の実施例におけるセキュリティシステムの構成の概要を表わしたものである。家屋１１１のドア１１２にはドアノブ１１３が取り付けられており、その下のドア部分にはキーホール１１４が設けられている。ドアノブ１１３の上側のドア部分には撮像用孔１１５と照明用孔１１６が開けられている。このセキュリティシステムでは、来訪者１１７がドア１１２のところまで来て、ドアノブ１１３に手を触れると、照明用孔１１６に内部から埋め込まれた赤外線ＬＥＤ（発光ダイオード）ランプ１１８が発光して、撮像用孔１１５の内部に配置された撮像素子（２次元ＣＣＤ）が来訪者１１７を撮影するようになっている。本実施例ではキーホール１１４が施錠用に使用される。

【００７１】図２は、ドアの要部を断面で示したものである。この実施例のドア１１２の外側に取り付けられているドアノブ１１３と内側に取り付けられているドアノブ１２１とは機構的に連動していない比較的簡易なタイプのものである。撮像用孔１１５はドア１１２の内側まで貫通しており、内側から画像ユニット１２２の筒状部１２２Ａが嵌入されるようになっている。筒状部１２２Ａは、ドア１１２の外側に面した箇所に単一あるいは複数枚のレンズから構成される光学レンズ１２３を配置しており、その焦点位置にデジタルカメラ等に広く使用されている２次元イメージセンサとしてのＣＣＤ（Charge Connected Diode：電荷結合素子）１２４を配置している。

【００７２】画像ユニット１２２の筒状部１２２Ａには画像出力部１２２Ｂが取り付けられており、この部分は

ドア１２２の内側の面に接着されている。画像ユニット１２２は一体構造となっているので、ドア１１２の外側からこれを取り外すことができないようになっている。ＣＣＤ１２４と画像出力部１２２Ｂの間の空間には、ＣＣＤ１２４から出力される画像を処理する画像処理回路１２５と、画像データを蓄積するメモリ１２６が収容されている。画像出力部１２２Ｂは、ドア１１２の内側から所望の時点で撮影を行うためのスイッチ１２７と、画像データを読み出すための画像データ出力端子１２８と、外側の画像あるいは蓄積された画像を表示する液晶ディスプレイ１２９から成っている。

【００７３】このうちＣＣＤ１２４には、たとえば６４０×４８０ピクセルのカラー画像を記録することができるものが使用されている。用途によっては更に高解像度のものを用意することもできる。画像処理回路１２５はＣＣＤ１２４から得られた画像データをメモリ１２６に記録するための画像処理を行うが、これと共に画像ユニット１２２全体の制御も行うようになっている。すなわち、画像ユニット１２２はドアノブ１１３および赤外線ＬＥＤランプ１１８と接続されており、ドアノブ１１３の電位変化を検出して、来訪者１１７がドアを開けようとこれに触れたときに赤外線ＬＥＤランプ１１８を発光させる。これと共にＣＣＤ１２４は被写体の画像を１枚あるいは予め定めた時間間隔で所定枚数撮影するようになっている。撮影によって得られた画像データはメモリ１２６に記憶される。赤外線ＬＥＤランプ１１８の発光に気がついて来訪者１１７がこれに目を向けるようなことがあれば、本人を特定するのに特に好都合な画像を取得することができる。

【００７４】メモリ１２６はたとえば１６メガバイト～１２８メガバイトの容量を持っいる。たとえば１６メガバイトのメモリ容量の場合には、６４０×４８０ピクセルのカラー画像を撮影日時を合成して１５０枚程度記憶することができる。メモリ１２６は画像処理回路１２５の制御の下で規定枚の画像データを記憶していき、これを超える画像データが入力される時点から古いものを１枚ずつ消去して、新しい画像データに置き換えるようにしている。

【００７５】画像ユニット１２２には、図示しない電源回路から電源が供給されるようになっている。電源回路はドア１１２に直接、商用電源あるいはこれを直流に変換した後の電源を引き込むようにしてもよいが、ドア１１２は開け閉めが行われるので、ヒンジ部分の電線の耐久性が問題となる。そこで本実施例のセキュリティシステムではドア１１２が閉まっている状態でドア１１２の内側表面に配置された図示しない受け側器具と接触する屋内電源側器具とが電磁結合を行って、電気エネルギをドア１１２内部の電源回路に供給するようになっている。この電源回路の内部には同じく図示しない容量の比較的大きなコンデンサあるいは二次電池が配置されており、画像ユニット１２２や赤外線ＬＥＤランプ１１８等の各部を駆動するための電源を供給するようになっている。もちろん、ドア１１２の内側から乾電池をセットしておくことも可能である。

【００７６】画像出力部１２２Ｂにはスイッチ１２７が付属しており、これを押すことによりＣＣＤ１２４を起動して、これによって得られた画像を表示すると共に、その画像をドアノブ１１３による検知の場合と同様にメモリ１２６に書き込むようになっている。画像データ出力端子１２８は、必要に応じてメモリ１２６内に格納されている画像データの読み出しを行う際に使用する出力端子である。この出力端子あるいはスイッチ１２７を操作しても、メモリ１２６の内容を消去することはできない。これは、家屋１１１（図１）に無断で侵入した者が画像を勝手に消去する事態の発生を防止するためである。したがって、スイッチ１２７が短時間内に押される回数を制限したり、１日に押される回数の上限を設けるようにすることも、一度撮影された画像を侵入者が勝手に上書きして消去する事態を防止するためには有効である。

【００７７】もっとも、このセキュリティシステムの最大の効果は、画像が撮像されて記録されることに気がついた侵入者等が、家屋への侵入等の所期の目的を達成することを断念して早期に立ち去るという犯罪の抑止効果にある。キーホール１１４に鍵を開ける道具を差し込んだ後、あるいは差し込む前にドアノブ１１３に手を触れたとき、赤外線ＬＥＤランプ１１８が発光するが、これに気づいた段階でその来訪者１１７の画像はすでに撮影されており、鍵を苦労して開ける前にその場から早々と立ち去らざるを得なくなるからである。夏等に風通しを良くするために、ドア１１２を少し開けているような場合にも、これを押し開けて入ろうとする時点ですでに撮影が行われてしまう。

【００７８】もちろん、家人も出入りの度に撮影される訳であるが、当人の場合には、撮られた画像が他人に利用される訳でもないので、何ら問題とならない。それどころか、子供が学校から一度帰って遊びに行ったのか、まだ全然帰って来ないのかというようなチェックが可能になる。また、留守をしているときに友人が訪ねてきたような場合にも、これを確認することができる。

【００７９】なお、実施例では来訪者１１７の検出をドア１１２の電位変化によって行っているが、光の反射あるいは遮断を検出する等の慣用の手法を用いて来訪者１１７を検出するようにしてもよい。また、呼び鈴やインターホン（ドアホン）が押されたときこれによって来訪者が来たことを判別して撮影を行うようにしてもよい。また、実施例では撮像用孔１１５と照明用孔１１６を設けたが、キーホールに似せた孔を設け、これらの内部にこのような部品をセットしてもよい。マイクロフォンやスピーカを配置する場合についても同様である。

【００８０】以上説明した本実施例では、既存のアパート等の家屋に家主等が僅かの費用をかけるだけで、高価な特殊な鍵を取り付ける以上の防犯効果を得ることができる。また、実施例では赤外線ＬＥＤランプ１１８を撮影に使用しているが、通常のＬＥＤ等の照明手段でもよい。また、周囲が明るい場所では照明用のランプを使用せずに撮影を行うことができる。また、長期に不在になるような場合には、通常のストロボのような発光がより明瞭に外部から分かる照明手段を使用することも有効である。

【００８１】第１の実施例の変形例

【００８２】図３は、本発明の第１の実施例の変形例としてのセキュリティシステムを屋内から見たものである。第１の実施例の図２と同一部分には同一の符号を付しており、これらの説明を適宜省略する。この変形例のセキュリティシステムでは、図示しないコンセントに接続された電源送信装置１４２がドア１１２側に取り付けられた電源受信装置１４１に電磁結合によって電源を供給している。電源受信装置１４１に接続された画像記録ユニット１２３Ａ内には先の実施例のような大容量のメモリは内蔵されておらず、撮影した画像は、画像記録ユニット１２３Ａに取り付けられたアンテナ１４３から屋内の所定の箇所に隠された受信装置１４４で受信され、ここで比較的大容量のメモリに順次格納されるようになっている。

【００８３】したがって、撮像装置に気がついた侵入者がドア１１２の全部または一部を壊すことによって画像記録ユニット１２３Ａを破損させたり、これを持ち去ることがあっても、その者の画像を安全に退避させることができる。また、受信側が比較的大容量のメモリを備えていれば、動画や高解像度の画像を充分な量、通信によって蓄えることができる。

【００８４】なお、画像記録ユニット１２３Ａ自体が携帯電話機等の無線端末に画像等のデータを直接配信することも可能であるし、受信装置１４４に所定のモード設定を行ったときにはこれが中継する形で携帯電話機等の無線端末に画像等のデータを配信するようにしてもよい。これにより、留守中の自宅に誰かが訪問するたびに、携帯電話機等でこれを把握することができる。したがって、画像記録ユニット１２３Ａ側にマイクロフォンやスピーカを配置しておけば、その者と必要な会話を行うことも可能になる。

【００８５】第２の実施例

【００８６】図４は、本発明の第２の実施例におけるセキュリティシステムの構成の概要を表わしたものである。本実施例で図１と同一部分には同一の符号を付しており、これらの説明を適宜省略する。

【００８７】本実施例ではドア１１２に改造を行うことが困難な者を対象にして、その付近の物品に来訪者の画像を撮影する装置を組み込むことにしている。この例では郵便ポスト１６１をそのための装置としているが、新聞入れ、呼び鈴あるいはドアホンのような物であってもよい。

【００８８】図５は、この例の郵便ポストの構成を示したものである。郵便ポスト１６１は郵便投函口１６２をその上部に有し、下部には郵便回収口１６３を有している。郵便回収口１６３には、必要に応じてキー１６４が取り付けられている。郵便ポスト１６１の郵便投函口１６２と郵便回収口１６３の間には、第１～第３の孔１６６～１６８が穿たれている。第１の孔１６６には赤外線ＬＥＤランプ１１８が取り付けられている。第２の孔１６７の内部には受光素子１６９が配置されている。第３孔１６８の内部には、図示しないがレンズと撮像素子が組み込まれている。これらは郵便ポスト１６１内部の画像処理ユニット１７１に接続されている。画像処理ユニット１７１は、郵便ポスト１６１内部の電池１７２から電源の供給を受けるようになっているが、可能であれば商用電源から電源を供給することもできる。画像処理ユニット１７１には送信アンテナ１７３が付属している。

【００８９】このような第２の実施例のセキュリティシステムでは、赤外線ＬＥＤランプ１１８が常時、あるいは間欠的に点灯し、受光素子１６９が受光レベルを検出することで郵便ポスト１６１の前に物体が現われたことを検出する。来訪者１１７があったような場合には、受光素子１６９がこれを検出し、画像処理ユニット１７１は前記した撮像素子を駆動して郵便ポスト１６１の前の画像を１枚ないし所定の時間間隔で複数枚取り込む。そして画像を１枚ずつ送信アンテナ１７３から送信する。

【００９０】送信された画像は、第１の実施例の変形例として図３で説明したと同様に家屋１１１内の受信装置１４４で受信され、ここで比較的大容量のメモリに順次格納されるようになっている。このとき、受信の日付も記録される。したがって、来訪者１１７が悪意を持った者のような場合で、何らかの異変に気付いて郵便ポスト１６１を破壊したり、あるいはこれを持ち去るようなことがあっても、来訪者１１７の画像が記録されているので、これに迅速に対処することができる。

【００９１】第３の実施例

【００９２】図６は、本発明の第３の実施例におけるセキュリティシステムの構成の概要を表わしたものである。この第３の実施例では金庫のセキュリティシステムを扱っている。金庫１８１はその扉１８２あるいはその周囲に第１および第２の孔１８３、１８４が穿たれている。また、金庫１８１の背後の部分には送信アンテナ１８５が取り付けられている。送信アンテナ１８５は金庫の外側のパネルを一部領域だけ非金属部分としてこの内部に組み込んでおいてもよい。これにより、送信アンテナ１８５を事前に破壊するという行為を防止させることができる。

【００９３】本実施例では第１および第２の孔１８３、

１８４の一方に赤外線ＬＥＤランプ等の発光手段を配置し、他方の孔の内部に光学系と撮像素子を配置している。また、金庫１８１の内部には第２の実施例で説明したと同様の画像処理ユニット１８６が内蔵されている。本実施例の画像処理ユニット１８６の場合には、電源供給用のコンセント１８７が備えられているが、金庫１８１の内部に充電池１８８が備えられているので、停電あるいはコンセント１８７が引き抜かれた場合にも所定時間の間は画像処理ユニット１８５に電源が供給されるようになっている。

【００９４】本実施例のセキュリティシステムの場合にも、所定の安全な場所（複数箇所であってもよい。）に配置された受信装置１４４（図３参照）が画像データを受信するようになっている。先の実施例と異なるのは、画像処理ユニット１８６は被写体を検知することなく、たとえば１分間隔で画像データを撮影している。これにより、１日の間に１５００枚ほどの画像が撮られて送信アンテナ１８５から順次受信装置１４４に送られることになるが、解像度を高くしてもこれらを格納する記憶媒体の容量はごく僅かで足りる。したがって、簡易な受信装置１４４で画像の管理を充分行うことができる。もちろん、コンピュータを使用して画像データを取り込むようにすれば、画像処理結果と連動した更に高度のセキュリティシステムを構築することができる。

【００９５】第３の実施例の第１の変形例

【００９６】図７は第３の実施例の第１の変形例として公衆トイレの防犯用のセキュリティシステムを表わしたものである。公衆トイレ２０１の男女別の入り口２０２、２０３の上には蛍光灯等の照明装置２０４、２０５が点灯しており、入り口２０２、２０３の複数箇所には撮影用の孔２０６～２０９が開けられている。これらの孔２０６～２０９の内部には前記したようなレンズと撮像素子が配置されている。また、公衆トイレ２０１の屋上等の所定の位置には送信アンテナ２１１が配置されていて、その電波が携帯電話機の無線基地局で逐次受信されるようになっている。役所等の公衆トイレ２０１の管理者側に備えられた記憶装置には、各所に配置された公衆トイレ２０１の画像データが逐次格納されている。

【００９７】もちろん、公衆トイレ２０１側に比較的大きなメモリ容量の記憶装置を配置して、これに画像データを順次蓄積するようにしたり、３０分とか１時間おきにこれらの画像データを無線基地局経由で公衆トイレ２０１の管理者側にまとめて送信することも可能である。

【００９８】第３の実施例の第２の変形例

【００９９】図８は第３の実施例の第２の変形例としてエレベータの防犯用のセキュリティシステムを表わしたものである。エレベータ２３１の出入り口あるいはその近傍に撮影用の孔２３２、２３３を開けておき、その内部にレンズと撮像素子等を配置しておくことで、無断侵入者を撮影し、間接的に無断侵入を防止することができる。画像の撮影は昇降用のボタン２３４の押下によって準備段階に移行し、ドアが開いて閉まるまでの時間について所定間隔で撮影を行うようにすればよい。エレベータ２３１の出入り口と対向する壁等にも撮像素子等を配置しておけば、事件があったような場合にどのような人物が何階から乗り込んで何階で降りたという事実を特定することができる可能性が高くなる。

【０１００】第４の実施例

【０１０１】図９はドアノブを使用したセキュリティシステムの要部を表わしたものである。第１の実施例のセキュリティシステムと異なるのは、ドア１１２の外側と内側でノブ２５１、２５２が連動したドアノブ２５３に本発明を適用している点にある。ドアノブ２５３はドア１１２と接触する部分に、押さえプレート２５５、２５６という金属板（台座）を取り付けるようになっている。したがって、押さえプレート２５５、２５６で隠れるだけの大きさの比較的大きな穴をドア１１２に開け、ドア１１２の外側に対応した押さえプレート２５５の背後に取り付けられた画像撮影処理ユニット２５７をドア１１２の内部空間に配置するようにする。画像撮影処理ユニット２５７は、キーロック機構２６０の存在しない空間を利用して配置されている。

【０１０２】画像撮影処理ユニット２５７の取り付けられた押さえプレート２５５には第１および第２の孔２５８、２５９が開けられている。第１の孔２５８には赤外線ＬＥＤランプ等の発光手段が組み込まれており、第２の孔２５９の背後の画像撮影処理ユニット２５７内には、図示しないレンズと撮像素子が組み込まれている。もう一方の押さえプレート２５６には、画像データ出力端子２６１が埋め込まれている。このような端子の代わりに画像撮影処理ユニット２５７内に画像データ送信用のアンテナが付属していてもよい。画像データ出力端子２６１を画像データの出力用に使用する画像撮影処理ユニット２５７は、画像データをある程度蓄積する必要があるので、その内部に比較的大容量の不揮発性のメモリが配置されている。この点は第１の実施例と同様である。

【０１０３】画像撮影処理ユニット２５７の電源は、前記した実施例と同様に電磁誘導によって外部の電源からエネルギを受け取る電源受信装置２６２から得ることができる。もちろん、ドア１１２に何らかの用途で電源が供給されている場合にはこれを使用することも可能である。

【０１０４】本実施例のセキュリティシステムの最大の特徴は、通常の家屋あるいはマンション等に多用されている形式のドアノブを用いるので、新築の際にこれを使用して簡易にセキュリティシステムを実現することができるだけでなく、本実施例のドアノブ２５３を購入して、今まで使用していたドアノブと交換するだけでセキュリティシステムを導入することができる点にある。特

に無線で画像データを送信するタイプのものでは、携帯電話機等の通信端末に来訪者の画像を送信することができる。また、すでに説明したようにマイクロフォンやスピーカを配置しておけば、その者と必要な会話を行うことも可能になる。

【０１０５】しかも、鉄等の金属で作られた通常のドアは防犯用に加工すること自体が困難であり、また美観を損ねる結果を招来することが多いが、本実施例のセキュリティシステムでは、ドアノブ２５３を交換するので、美観を損ねるおそれがない。

【０１０６】第４の実施例の変形例

【０１０７】図１０は、本実施例を自動車に応用したセキュリティシステムの概要を表わしたものである。自動車２８１もその外部が金属で作られており、防犯用に特別に加工すると美観を損ねるおそれがある。しかしながら、ドア２８２、２８３を開けるときに必要なドアの把手２８４、２８５自体に直接、あるいはドアの把手２８４、２８５の付属装置２８６、２８７にすでに説明したような孔を開けておき、この部分を使用してドア２８２、２８３を開ける人を撮影するようにすれば、ドアの把手２８４、２８５あるいはその付属装置２８６、２８７を交換することでセキュリティシステムを導入することができる。

【０１０８】この変形例の場合にも、自動車２８１に近接し、あるいはドアの把手２８４、２８５等に接触した時点で、あるいは所定の時間間隔でドアの把手２８４、２８５の近傍の画像が１枚ずつ撮られるので、自動車２８１の盗難は事実上困難になる。画像データを自動車２８１内部に蓄積するか、図７で説明したような無線を使用して所定箇所に送信するかは自由であるが、自動車２８１自体を盗まれる場合を想定すると、無線を使用して画像を携帯電話機や所定の管理サーバ上に送信しておく方が有効である。

【０１０９】またこの変形例ではドアの把手２８４、２８５あるいはこれらの付属装置２８６、２８７の内部に撮像素子等を配置することにしたが、バックミラー等の他の部品の内部に撮像素子等を配置することができれば、同様に本発明を適用することができる。また、鍵自体がドアの把手２８４、２８５自体に取り付けられていないような場合には、その鍵と一体的に撮像素子等を配置することも可能である。

【０１１０】第５の実施例

【０１１１】図１１は本発明の第５の実施例のセキュリティシステムの概要を表わしたものである。このシステムは、自転車３０１、自動車３０２、バイク３０３等の各種交通機関を駐車する駐車場（もちろん、自動車３０２とか自転車３０１のいずれか１種類の交通機関のみを駐車あるいは駐輪するものであっても可能。）で使用されるものである。この例で自転車３０１、自動車３０２、バイク３０３は、それぞれ先の実施例の変形例で説明したドアの把手やボディの所定箇所あるいはハンドル、外付けのスピードメータ等に人の接近や接触を検知する検知手段と撮像装置を備えている。駐車場３０４には、これらの交通機関で共通使用される受信装置３０５が設置されている。駐車あるいは駐輪している自転車３０１、自動車３０２、バイク３０３等の各種交通機関は人の接近や接触を検知すると、自己のＩＤと共に撮影した画像データを受信装置３０５に送信するようにしている。受信装置３０５は比較的大容量のメモリを備えており、受信した画像データをＩＤ別に区分けして記憶するようにしている。

【０１１２】したがって、盗難やいたずらが発生すると、駐車場３０４の管理者に通知して画像を読み出してもらうことにより、事故の発生日時とこれに係わった可能性のある人物の画像を入手することができる。もちろん、受信装置３０５を介して所有者の通信端末に必要な画像を中継する契約を行うことも可能である。

【０１１３】同様のシステムは、ボート等の船舶や集合住宅を管理する場所でも適用することができる。また、インターネットを利用してウェブ・サーバで一括管理することもできる。

【０１１４】第６の実施例

【０１１５】図１２は本発明の第６の実施例のセキュリティシステムの概要を表わしたものである。ここでは、絵画の展示場で適用されるシステムを表わしている。それぞれの絵画３２１、３２２の前には鑑賞者３２３の接近を検知してその画像を撮影し送信する撮像送信ユニット３２４が取り付けられている。撮像送信ユニット３２４は、壁に直接埋め込まれていてもよい。各撮像送信ユニット３２４の送信した画像データは館内の受信装置３２５が受信して、その比較的大容量のメモリにサイクリックに書き込んで、容量が越えた時点で古い画像を上書きするようになっている。入場者が多い場合には、３０秒おきというように所定の時間間隔で画像データを読み込んで送信するモードに設定しておいてもよい。また、異常な行動（画像の動き）が管理者側あるいは画像の差分データをとる装置等で察知された場合には、画像を高解像度に切り替えたり、動画モードに切り替えるようにしてもよい。

【０１１６】このように本発明はドアあるいは扉に用途が限定されるものではなく、動産全体、不動産の一部としての所定の空間あるいは通路に対しても適用することができる。撮像された画像は順次格納しておき、メモリ容量が少ないときには古い画像データに上書きしていくようにすることで、システムの実効性を高めることができる。しかも悪意の者が撮影に気付いたときにはすでにその画像が安全な場所に格納されていたり、遠隔地等に送信されているので、所期の目的を達成させることなく退散させるといった効果がある。

【０１１７】第７の実施例

【０１１８】図１３は本発明の第７の実施例のセキュリティシステムの概要を表わしたものである。この図で図１と同一部分には同一の符号を付しており、これらの説明を適宜省略する。本実施例では、ドア１１２に電子式錠装置４０１が取り付けられており、その上部にセキュリティ装置４０２が取り付けられている。電子式錠装置４０１にはドアノブ４０３とキー溝４０４が取り付けられている。電子式錠装置４０１はキー溝４０４に差し込む図示しないキーによって開錠することができる他、セキュリティ装置４０２の指示によっても開錠することができるようになっている。

【０１１９】本実施例のセキュリティ装置４０２は後に説明するように独自のアドレスを有する無線端末としての機能を有しており、最寄の基地局４１１に対して発呼できるようになっている。ただし、基地局４１１を介して他の無線端末あるいは固定式電話等の端末から発呼することはできない。すなわち、セキュリティ装置４０２は自ら発呼して接続した端末との間でのみ通話やデータの交換を行うことができる。これは、セキュリティ装置４０２が悪意の第三者の指示によって電子式錠装置４０１に開錠の指示を与えることを防止するためである。

【０１２０】基地局４１１は通信網４１２を介して他の基地局４１３（図では代表的に１つのみを表示している。）やセキュリティ管理会社４１４と接続されている。図ではセキュリティ管理会社４１４が通信網と有線で接続されている形を示しているが、無線で接続されていてもよいし、インターネット網等の他の通信網を介して接続されていてもよい。ここで携帯電話端末４１５はセキュリティ装置４０２の所持者の端末であるとする。

【０１２１】図１４は、本実施例のドアの要部の断面構造を表わしたものである。ドア１１２に組み込まれたセキュリティ装置４０２は、図２で示した実施例のように単一あるいは複数枚のレンズから構成される光学レンズ１２３と、２次元イメージセンサとしてのＣＣＤ１２４を備えている。また、光学レンズ１２３の上方にはスピーカ部４２１が配置され、下方にはマイク部４２２と赤外線ＬＥＤランプ１１８が配置されている。スピーカ部４２１、マイク部４２２および赤外線ＬＥＤランプ１１８の後ろ側のスペースには制御部４２３が配置されている。制御部４２３は画像処理だけでなく、通信制御や音声の入出力および電子式錠装置４０１の制御も行うようになっている。セキュリティ装置４０２の背後には無線アンテナ４２５が取り付けられており、また電子式錠装置４０１との間には制御信号線４２６が取り付けられている。セキュリティ装置４０２の電源は、図３に示した第１の実施例の変形例のようにして取得してもよいし、電子式錠装置４０１から図示しない電源ラインを使用して取得してもよい。なお、無線アンテナ４２５は図１４に示したようにドア１１２内部に配置してもよいし、他の場所まで無線用の信号線を延長して、電波の送受信に良好な場所に配置するようにしてもよい。

【０１２２】図１５は、本実施例における電子式錠装置の開錠制御の様子を表わしたものである。本実施例では、たとえば幼少の子供が家に帰ってきたときに親等がこれを確認して、家の内部に入るための鍵を開けることができる。店の従業員を確認後に店内に入れたり、来客が来る予定のときに突然外出してしまい、とりあえずその来客を家または事務所の内部に通すような場合にも本実施例が有効である。本実施例ではこれらの者を他の実施例と同様に来訪者１１７と総称する。

【０１２３】図１３または図１４に示したセキュリティ装置４０２あるいは他の周知の装置がドア１１２の付近に現われた来訪者１１７を検知すると（ステップＳ４５１：Ｙ）、撮影を行った後、「撮影を行わせていただきました」等の音声がスピーカ部４２１から流れて（ステップＳ４５２）、悪意の来訪者を立ち退かせる処理が行われる。この後に再度、来訪者１１７がドア１１２の前にいるかどうかを検知して（ステップＳ４５３）、いなくなれば（Ｙ）、処理を終了させる（エンド）。

【０１２４】この状態でも来訪者１１７が依然として検知されていれば（ステップＳ４５３：Ｎ）、図１４に示した制御部４２３は予め指定したその家の主人等の携帯電話機等の携帯電話端末４１５へ発呼する（ステップＳ４５４）。その後、時間t_1以内に指定端末としての携帯電話端末４１５との通話が可能になれば（ステップＳ４５５：Ｎ、Ｓ４５６：Ｙ）、その携帯電話端末４１５から開錠を指示する信号が到来した時点で（ステップＳ４５７：Ｙ）、制御部４２３は開錠指示信号を制御信号線４２６を介して電子式錠装置４０１に送り、開錠処理を行う（ステップＳ４５８）。この場合、電子式錠装置４０１は所定時間経過後に再び自動的に施錠する。その携帯電話端末４１５が開錠を指示するには、所定のパスワードを入力することを条件にしてもよい。開錠指示信号が到来することなく通信が終了した場合には（ステップＳ４５９：Ｙ）、一連の処理が終了する（エンド）。

【０１２５】なお、携帯電話端末４１５の所有者は、開錠指示信号を送信する前にＣＣＤ１２４の画像を受信しており、またスピーカ部４２１やマイク部４２２を通じて来訪者１１７と会話して、開錠を行う必要のある者であるかどうかを十分確認することができる。また、単なるセールスマン等の開錠を行う必要のない者に対しては、通話によって必要な処理を行うことができる。

【０１２６】一方、子供が家に帰ってきて鍵を開けてもらうような場合に、携帯電話端末４１５の所有者がたまたま通話を行えないエリアにいるような場合も考えられる。そこで、本実施例ではステップＳ４５５で時間t_1が経過しても携帯電話端末４１５の所有者と通信ができないとき（着呼できないときも含む）、その所有者が転送モードを設定しているかどうかを確認する（ステップＳ４６０）。転送モードに設定されていない場合には

（Ｎ）、一連の処理が終了する（エンド）が、設定されている場合には（Ｙ）、図１３に示したセキュリティ管理会社４１４へその通話先が変更される。なお、セキュリティ管理会社４１４への転送の前に、母親の代わりに父親の携帯電話機というように他の者に転送が行われるようにしてもよい。

【０１２７】セキュリティ管理会社４１４が着呼すると（ステップＳ４６１）、先の携帯電話端末４１５の所有者と同様に専門のスタッフが来訪者１１７と通話を行ったり、画像を確認して、予め指定された子供のように確かな者に対しては開錠信号を代行して発信する。セキュリティ装置４０２は、開錠信号が到来したら（ステップＳ４６２：Ｙ）、すでに説明したように開錠処理に進み（ステップＳ４５８）、通信が終了したら（ステップＳ４６３：Ｙ）、すべての処理を終了させることになる（エンド）。

【０１２８】なお、セキュリティ管理会社４１４は開錠の処理を行ったり、来訪者と話をしたような場合には、これを電話で携帯電話端末４１５の所有者に通知したり、その内容のメールを出すことも有効である。

【０１２９】このように本実施例ではセキュリティ装置４０２が発呼したその通信中に開錠信号が到来したときのみ、このセキュリティ装置４０２から電子式錠装置４０１に対して開錠の指示がでる。したがって、他の場所から開錠を指示する信号を送ってきて開錠を行う場合と異なり、セキュリティが極めて高くなる。しかも来訪者１１７は撮影されるので、この点でも悪意の来訪者に対するセキュリティが高い。

【０１３０】図１６は、悪意の来訪者が撮影を妨害する場合の対策としての処理の流れを表わしたものである。この処理は、本実施例に限らず先の各実施例でハードウェアを工夫することで同様に実行することができる。図１４に示したＣＣＤ１２４は時間t_2ごとにドア１１２の前を撮影している（ステップＳ４７１、Ｓ４７２）。そして、撮影が行われるたびに特定の複数の画素から得られる画像の明るさ、あるいは全体の画像の明るさを前回のもの、あるいは前回の複数回分のものと比較するようにしている（ステップＳ４７３）。比較された結果、明るさの差が予め定めた許容値以内の場合には（ステップＳ４７４：Ｙ）、特に異常が発生していないものとしてステップＳ４７１の処理に戻る。

【０１３１】ところで、悪意の者が自分が撮影されるのを嫌って、図１４に示す光学レンズ１２３にガムテープのようなものを貼り付けて撮影ができないようにすることが考えられる。このような場合には、ＣＣＤ１２４に到達する画像の明るさが急激に減少する。また、人によっては懐中電灯等の光の出るものをＣＣＤ１２４の前に配置して、明るさを維持しながら犯行を企む場合がある。更に光学レンズ１２３を破壊するようなこともある。このような場合には、いずれにせよＣＣＤ１２４が得る画像の明るさが変化する。

【０１３２】このように明るさの差が予め定めた許容値を越えるような場合には（ステップＳ４７４：Ｎ）、制御部４２３はスピーカ部４２１を制御して警報音を所定時間、たとえば１０秒間出力する（ステップＳ４７５）。この後に、再度、ＣＣＤ１２４による撮影が行われて（ステップＳ４７６）、その画像の明るさが基準値の範囲内であるかどうかのチェックが行われる（ステップＳ４７７）。ここでの基準値の範囲はステップＳ４７４の範囲であってもよいし、ステップＳ４７４の処理による誤動作を防止するために予め設定されている値の範囲内であってもよい。基準値の範囲内であれば（Ｙ）、悪意による撮影の妨害が解消したものとして、ステップＳ４７１の処理に戻る。ただし、装置によっては撮影した画像を解析し、ドア１１２の前の通常得られる画像と異なる場合には「基準値の範囲」外としてもよい。

【０１３３】ステップＳ４７７で基準値の範囲外とされた場合には（Ｎ）、セキュリティ装置４０２が指定端末としての携帯電話端末４１５に発呼する（ステップＳ４７８）。これにより、携帯電話端末４１５側では音声で通話する等により状況を確かめ、必要に応じて警察に通報する等の処置を採ることができる。携帯電話端末４１５側が通話をすることができないような場合等にはセキュリティ管理会社４１４に転送され、あるいはこれを宛先として発呼が行われることも可能である。

【０１３４】第８の実施例

【０１３５】図１７は本発明の第８の実施例のセキュリティシステムの概要を表わしたものである。このセキュリティシステムは、自動車４０１の運転席の上方に配置された広角の撮像装置４０２と、後部座席の上方に配置された温度検出器４０３、マイクロフォン４０４、スピーカ４０５、非常ボタン４０６および無線送受信器付制御装置４０７とにより構成されている。このうち、温度検出器４０３、マイクロフォン４０４、スピーカ４０５、非常ボタン４０６および無線送受信器付制御装置４０７は１つの筐体内に納められていてもよい。もちろん、撮像装置４０２も含めて全体を一つの比較的小さな筐体内に格納することも可能である。この場合、携帯電話機にＣＣＤ撮像装置と温度検出器が組み込まれたようなものを想定すればよい。

【０１３６】図１８は無線送受信器付制御装置の制御の概要を表わしたものである。無線送受信器付制御装置４０７は予め定められた１または複数の携帯電話機等の通信端末の受信端末として動作すると共に、特定の場合にはこれら１または複数の携帯電話機等の通信端末に対して所定の優先度をもって発呼できるようになっている。

【０１３７】前記した１または複数の携帯電話機等の通信端末が発呼して、所定の操作によってモニタオン信号を送信してくると（ステップＳ４２１：Ｙ）、ＣＰＵ（中央処理装置）を内蔵した無線送受信器付制御装置４

０７は画像・音声通信モードに移行し（ステップＳ４２２）、撮像装置４０２で静止画あるいは動画を撮影してこの通信端末に送信すると共にマイクロフォン４０４およびスピーカ４０５を動作状態にして、音声あるいは車内の音を送信状態にすると共に、通信中の通信端末から送られてきた音声信号による音声をスピーカ４０５から出力する。したがって、その通信端末は車内の者と通話を行うことができる。画像・音声通信モードの解除は、その通信端末がモニタオフ信号を送信してこれが無線送受信器付制御装置４０７側で受信されることによって行われる（ステップＳ４２３）。

【０１３８】一方、車内の温度が予め設定した温度よりも高い異常な状態になったとき（ステップＳ４２４：Ｙ）、あるいは非常ボタン４０６が押されたとき（ステップＳ４２５：Ｙ）、無線送受信器付制御装置４０７は前記した通信端末に発呼する（ステップＳ４２６）。このような通信端末が複数存在する場合には最優先のものに発呼し、これが応答しないときには次の優先順位の通信端末に対する発呼に切り替わる。予め定められた通信端末が３つ以上存在する場合には、接続が行われないたびに順次下位の通信端末に切り替わる。通信端末の中には先の実施例の図１３で示したようなセキュリティ管理会社が含まれていても良い。

【０１３９】相手の通信端末と通信できる状態になったら、ステップ４２２に移行して画像が送信され、音声で通話ができる状態になる。この画像・音声通信モードの解除は、通信中のその通信端末がモニタオフ信号を送信することで行われるが、車内の者が図示しないリセットボタンを押せば通信が強制終了する。

【０１４０】この第８の実施例のセキュリティシステムによれば、たとえば車内に子供が取り残されたり、うっかり置き忘れたような場合で温度が異常に上昇したとき、親等の通信端末が自動的に呼び出され、車内の様子が伝達される。また、車内で何らかの異常が発生したような場合には、非常ボタン４０６を押すことで車外の者にこれを通知することができる。たとえば強盗が車内に押し入ったような場合には、自分の携帯電話機をオフにして非常ボタン４０６を押せば、自分の携帯電話機よりも下位の優先順位の親元等に車内の状況を把握させることができ、救助を求めることができる。また、先の実施例でも説明した自動車内の不法侵入に対しても、ドアの外を撮影するだけでなく本実施例によって車内の撮影を開始させることで、その者の特定に貢献することができる。この意味では特に撮像装置４０２は車内の目立たない位置に最初から組み込まれていることが望ましい。このような場所のとしては、エアーコンディショナの送風口やスピーカの孔を一例として挙げることができる。

【０１４１】なお、第７の実施例等では無線で異常等の通信を行ったが、固定式電話機のように有線でこれらの通信を行うことも可能である。また、各実施例ではレンズとＣＣＤを１組配置することにしたが、これらを複数組配置するようにしてもよい。この場合には、他人の悪意あるいは装置の故障によりそのうちの１つの撮影ができないような事態が発生しても、撮影を行うことができる。特に、第７の実施例のような構成とすれば、１つの撮像系に異常が検出されたときに残りの撮像系で撮影すると共に、必要に応じて所定の宛先に連絡を行うことができる。したがって、たとえば自動車の盗難や家屋の侵入といった事態の発生時に迅速に対処することができると共に、有力な証拠を取得することも可能になる場合がある。

【０１４２】第９の実施例

【０１４３】図１９は本発明の第９の実施例のセキュリティシステムの概要を表わしたものである。本実施例のセキュリティシステムでは、自動車の運転席前方のボード５０１上におけるキー挿入口５０２のすぐ上にスピーカの音声出力用の複数の孔の集合体５０３が配置されている。このうちの中央の比較的大きな孔５０４の内部には、たとえば第７の実施例で説明したドア１１２の光学レンズ１２３およびＣＣＤ１２４の組み合わせからなる撮像装置５０５が配置されている。また、ボード５０１内部で撮像装置５０５の側方あるいは背後には、音声出力用のスピーカ５０６が配置されている。更に、キー挿入口５０２の背後には音声を採取するためのマイクロフォン５０７およびエンジン始動検出回路５０８が配置されている。エンジン始動検出回路５０８は、キーの回転位置を図示しないマイクロスイッチ等の機械的なセンサで検出するようなものであってもよいし、実際にエンジンが始動したことを自動車の制御回路が判別したことによる信号をそのまま利用してもよい。

【０１４４】撮像装置５０５、スピーカ５０６、マイクロフォン５０７およびエンジン始動検出回路５０８は、同じくボード５０１の内部に配置された装置内通信端末５１１と接続されている。装置内通信端末５１１はカメラ内蔵携帯電話機のカメラを取り除いた本体部分とほぼ同様の構成となっており、車内の図示しない電源装置から電源の供給を受けるようになっている。この装置内通信端末５１１はこれを搭載した自動車の所有者の携帯電話機５１２とは異なった電話番号を有しており、単独で最寄りの無線基地局５１３ならびにその通信ネットワーク５１４を経由して予め設定した相手にデータの送信を行うことができるようになっている。

【０１４５】携帯電話機５１２は全く通常の携帯電話機であるが、装置内通信端末５１１と対の関係を持っている。対の関係は、携帯電話機５１２側あるいは装置内通信端末５１１から他方の装置に設定するものであり、設定内容は双方の電話機（通信端末）の図示しないＲＯＭ（リード オンリ メモリ）内に格納される。本実施例ではこのように装置内通信端末５１１と対の関係を持っている携帯電話機５１２を特定携帯電話機５１２と呼ぶこ

とにする。

【０１４６】図２０は、本実施例で自動車の所有者あるいは第三者がこの自動車を運転するためにキーを差し込んだ場合の装置内通信端末の制御の様子を表わしたものである。装置内通信端末５１１の図示しないＣＰＵは、エンジン始動検出回路５０８がエンジンの始動を検出すると（ステップＳ５３１：Ｙ）、撮像装置５０５を駆動して運転席でキーを操作した者の画像を記録する（ステップＳ５３２）。この画像は比較的短時間の動画であってもよいし、静止画を複数枚撮影するものであってもよい。複数の孔の集合体５０３に方向を変えて複数の撮像装置５０５を組み込むことができ、この場合には各種の方向の画像を撮影することができる。したがって、キーを挿入した者を特定する画像をこのうちの幾つかに収めることのできる可能性が高い。この意味では運転席を見渡せる位置であってキー挿入口５０２から比較的離れた位置に更に撮像装置を配置したり、もともと撮像装置を独自の観点から１または複数組、車内の所望の位置に配置しておくことも有効である。

【０１４７】このようにして画像の撮影および記録が行われたら、ＣＰＵはこの自動車の内部または近くに所有者の携帯電話機が存在するかどうかを判別する。この判別のために装置内通信端末５１１は特定携帯電話機５１２に対して電話を掛ける。そして特定携帯電話機５１２が同一の無線基地局５１３の受信エリアに存在する場合には近くに存在するものと判別して（Ｙ）、その時点で通話を終了させる（リターン）。したがって、特定携帯電話機５１２によっては着信音が鳴動する。

【０１４８】装置内通信端末５１１は特定携帯電話機５１２が同一の受信エリアに存在しないことを判別したら（ステップＳ５３３：Ｎ）、先に撮影した画像を現在の位置情報と共に特定携帯電話機５１２に対して送信する（ステップＳ５３４）。このとき、撮影日時に関する情報も送られる。ただし、特定携帯電話機５１２がＧＰＳ（Global Positioning System：全地球測位システム）等の位置検出手段を備えていない場合には、撮影した画像とその撮影日時のみが送信されることになる。

【０１４９】したがって、いずれかの者がキーを用いて無断に自動車のエンジンを始動させた場合には、特定携帯電話機５１２に対してこの画像やその他のデータが送られてくることになる。自動車の所有者は送られてきた画像によって、これが家族等の正当な権限を有する者の乗車であるかどうかを容易に判別することができる。また、場合によってはこの者とスピーカ５０６およびマイクロフォン５０７を用いて会話をして確認を行うことができる。

【０１５０】これにより、その自動車の発進に問題がないとされる場合、特定携帯電話機５１２の所有者は所定のキースイッチを押下して所定の終了通知を装置内通信端末５１１に対して送出する。装置内通信端末５１１はこの終了通知を受信すると（ステップＳ５３５：Ｙ）、一連の送信処理を終了させる（リターン）。このような終了通知が受信されない場合、装置内通信端末５１１は時間ｔが経過するたびに（ステップＳ５３６：Ｙ）、同様に運転席の画像を記録して（ステップＳ５３７）、ステップＳ５３４に戻りこれを特定携帯電話機５１２に対して送信する処理を繰り返す。したがって、第三者が勝手にその自動車を発進させたような場合には、その第三者が運転を行っている間、その画像を特定携帯電話機５１２に対して送信することができる。装置によっては、通信状態を継続させて運転席の画像を順次送信するようにしてもよい。

【０１５１】なお、本実施例では撮像装置５０５、スピーカ５０６、マイクロフォン５０７を配置したが、これらの一部または全部を省略しても特定携帯電話機５１２に対してその者の所有する自動車が無断に発進される事態を迅速に通知することができる。また、実施例では装置内通信端末５１１が特定携帯電話機５１２に対して通常の発信を行ったが、同一サービスエリア内で内線通話を行える場合には内線通話を試みて、通話が成立したときに特定携帯電話機５１２が近くに存在するものと判別してもよい。

【０１５２】第９の実施例の変形例

【０１５３】図２１は本発明の第９の実施例のセキュリティシステムの変形例としての特定携帯電話機のセキュリティシステムの要部を表わしたものである。この変形例の特定携帯電話機５１２Ａは着脱自在の近距離通信カード５５１をセットしている。この近距離通信カード５５１は所定のＩＤの端末から返答要求があると、これに対して返答用の電波を自己のＩＤと共に一定時間だけ出力するようになっている。もちろん、このような近距離通信カード５５１と同様の機能を有する回路が予め特定携帯電話機５１２Ａの内部に一体として組み込まれていてもよい。

【０１５４】一方、自動車側にセットされている装置内通信端末５１１Ａは、運転のためのキーが図１９に示したキー挿入口５０２に挿入されてエンジンの始動のための操作が行われたとき、所定時間にわたって自己のＩＤと返答要求を送出するようになっている。この装置内通信端末５１１Ａおよび特定携帯電話機５１２Ａの送出するこれらの電波は遠くにまで届くことの無い微弱な強さである。

【０１５５】図２２は、この変形例における装置内通信端末側の処理の流れを示したものである。装置内通信端末５１１Ａ内の図示しないＣＰＵは、第９の実施例で説明したエンジン始動検出回路５０８がキーの操作によるエンジンの始動を検出すると（ステップＳ５７１：Ｙ）、自己のＩＤと返答要求信号を送信する（ステップＳ５７２）。これらの信号は無線基地局５１３に送出されるような強い電波ではない。特定携帯電話機５１２Ａ

がその自動車内あるいはその自動車の近辺に存在する場合にはこれらの電波を受信する。そこで、前記したように特定携帯電話機５１２ＡはそのＩＤをチェックして対応関係にある装置内通信端末５１１Ａのものであれば自己のＩＤを付した返答信号を出力する。この返答信号も無線基地局５１３に送出されるような強い電波ではない。

【０１５６】装置内通信端末５１１Ａは、返答信号を受信したら（ステップＳ５７３：Ｙ）、これに含まれているＩＤが装置内通信端末５１１Ａと対の関係にあるものとして予め登録されたＩＤであるかどうかをチェックし（ステップＳ５７４）、登録されたＩＤであれば一連の処理を終了させる（エンド）。

【０１５７】これに対して、ステップＳ５７３で返答信号が送り返されてこなかったり（Ｎ）、あるいは返答信号自体は装置内通信端末５１１で受信されてもそのＩＤが登録された内容と一致していなかったような場合には（ステップＳ５７４：Ｎ）、第三者がキーを操作した可能性がある。そこでこの場合には、装置内通信端末５１１が特定携帯電話機５１２Ａに対して電話を掛けることになる（ステップＳ５７５）。この際に、撮影が行われていればその画像を送信してもよいことはもちろんである。

【０１５８】このようにこの変形例では、自動車のエンジンを始動させるときにその近くに所有者の携帯電話機が存在する場合に無線基地局５１３を介しての所有者への発信を控えるようにした。このため、自動車の所有者がキーを操作してエンジンを始動させるたびに通信費の出費を強いられるということがなくなる。また、変形例では独自の電波を利用して装置内通信端末５１１Ａが特定携帯電話機５１２Ａの存在の有無を判別するので、その電波の強弱や感度を調整することで、装置内通信端末５１１Ａと特定携帯電話機５１２Ａの間の感知できる距離をある程度自在に調整することができる。したがって、実施例ではコンビニエンスストアに買い物に立ち寄った場合に自動車の盗難に合う可能性があるが、この変形例では特定携帯電話機５１２Ａを車外に持ち出した状態で特定携帯電話機５１２Ａの検知できる範囲外とすることができる。

【０１５９】第１０の実施例

【０１６０】図２３は本発明の第１０の実施例のセキュリティシステムの要部を表わしたものである。この実施例では、先の実施例の図１と同様にドア１１２におけるドアノブ１１３の上側に撮像用孔１１５が配置されているだけでなく、集合住宅における部屋番号や居住者を示したプレート５９１の透明部分あるいは半透明部分の裏側に別の撮像用孔５９２が設けられている。これにより、来訪者の背が高かったり、ドアノブ１１３の位置が比較的低い位置であった場合にも、その者の画像を正確に捕らえる確率が高くなる。

【０１６１】このように来訪者の顔または姿を画像として正確に捕らえるためには、撮像用の装置のレンズを比較的広角のものにするか、ドアまたはその近辺だけでなく複数の場所から来訪者を捕らえるようにするか、あるいは１つの場所からのみ画像を捕らえる場合にはレンズを複数の場所を向くように光学機構を回転させるといった手法が有効である。光ファイバを使用して複数箇所で得られた画像を１つのＣＣＤに導いてそれぞれの分担領域に画像を結像させ、分割画像として記録することも可能である。

【０１６２】これに対して、図１０に示した自動車のドアの場合には、複数のドアの把手２８４、２８５等に対応して撮像装置を配置しておき、１つについて何らかの異変が生じたときに残りの撮像装置も一斉に画像を撮影するようにすると、画像の撮影範囲をある程度重複させておけば、撮影対象をより確実に画像に収めることができる。

【０１６３】なお、第９の実施例では自動車を例にして説明したが、船舶、ケーブルカー、飛行機等の交通機関であって、その走行のための動力源のオン・オフをキーによって制御するその他の交通機関についても本発明を同様に適用することができる。また、実施例ではキーを用いてエンジンを始動させる場合を説明したが、ボンネットを開けて配線を変える等によってエンジンを始動させるような場合にも、エンジンの始動時に特定通信端末が周囲に存在するかどうかを判別することによって、悪意の第三者による交通機関の盗難等を早期に解決することができる。

【０１６４】

【発明の効果】以上説明したように請求項１記載の発明によれば、撮像手段および撮像データ記憶手段が扉あるいはその近傍に埋め込まれるので、自分が撮影されたことに気づいた侵入者等は撮影された画像を消去したり撮像データ記憶手段自体を取り出すことが困難であり、早急に現場を立ち去ることになり、無断侵入や盗難あるいは不正行為の発生を有効に防止することができる。また銀塩写真と比べてランニングコストをわずかに抑えることができ、また事件が起きたときには画像データを有効な資料とすることができる。

【０１６５】また請求項２記載の発明によれば、撮像手段のみならず撮像データ発信手段も扉あるいはその近傍に埋め込まれているので、発信を安全に行うことができる。しかも本発明の場合には画像自体は所定の受信先に送られてしまうので、仮に撮像手段や撮像データ発信手段が持ち去られたとしても、画像の記録は残ることになり、結果的に無断侵入や盗難あるいは不正行為の発生を有効に防止することができる。

【０１６６】更に請求項３記載の発明によれば、小型化された撮像のための装置をドアノブあるいはこのドアノブとドアとの間に配置されたドアノブの台座の孔から撮

影することにしたので、ドア自体を加工する必要がなく有効なセキュリティシステムを実現することができる。またドアノブを交換する場合もドアを取り替えて改造を行う場合に比べると遙かに安価であり、経済的なシステムを構成することができる。更に、台座の表面に凹凸を付けるといったようにデザインを工夫すれば、孔の存在を判りにくくすることができる。

【０１６７】また、請求項４記載の発明によれば、小型化された撮像のための装置をドアノブあるいはこのドアノブとドアとの間に配置されたドアノブの台座の孔から撮影することにしたので、ドア自体を加工する必要がなく有効なセキュリティシステムを実現することができる。またドアノブを交換する場合もドアを取り替えて改造を行う場合に比べると遙かに安価であり、経済的なシステムを構成することができる。しかも撮像データ発信手段は、トリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する。したがって、事故の発生や友人等の来訪を迅速に知ることができる。更に、台座の表面に凹凸を付けるといったようにデザインを工夫すれば、孔の存在を判りにくくすることができる。

【０１６８】更に請求項５記載の発明によれば、自動車、船等の交通機関のドアの外側部分に突出して取り付けられたドアの把手あるいはこの把手に取り付けられた付属部品に孔を穿つので、ドア自体を加工する必要がない。したがって、現在使用している交通機関を簡単に改造することができ、無断侵入や盗難あるいは不正行為の発生を有効に防止することができる。

【０１６９】また請求項６記載の発明によれば、自動車、船等の交通機関のドアの外側部分に突出して取り付けられたドアの把手あるいはこの把手に取り付けられた付属部品に孔を穿つので、ドア自体を加工する必要がない。したがって、現在使用している交通機関を簡単に改造することができ、無断侵入や盗難あるいは不正行為の発生を有効に防止することができる。しかも撮像データ発信手段は、トリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信するので、その交通機関自体が盗難にあった場合も画像データ自体は安全な箇所に保持されることになり、盗難等に関係した者の特定が容易になる。

【０１７０】更に請求項７記載の発明によれば、交通機関の外側に予め荷物を止めるための部品やバックミラー等の部品が配置されている場合には、これらの部品の内部に撮像手段等を収容することで、本発明による盗難防止等の利益を得ることができる。

【０１７１】また請求項８記載の発明によれば、交通機関の外側に予め荷物を止めるための部品やバックミラー等の部品が配置されている場合には、これらの部品の内部に撮像手段等を収容することで、本発明による盗難防止等の利益を得ることができる。しかも本発明では撮像データ発信手段を配置しているので、画像データ自体は安全な場所に送信され、かつ画像データを早期に取得できることになる。

【０１７２】更に請求項９記載の発明によれば、撮像手段が通路または部屋の壁に埋め込まれ壁の前の被写体を撮像することができるようになっているので、特別の通路や部屋を有効に監視することができる。

【０１７３】また請求項１０記載の発明によれば、撮像手段が通路または部屋の壁に埋め込まれ壁の前の被写体を撮像することができるようになっているので、特別の通路や部屋を有効に監視することができる。しかも本発明では撮像データ発信手段を配置しているので、画像データ自体は安全な場所に送信され、かつ画像データを早期に取得できる。

【０１７４】更に請求項１１記載の発明によれば、郵便受けやドアホン等のように人の出入りする扉または通路の周辺に配置された防犯以外の所定の用途に使用される容器に孔を穿ち、撮像手段でこの孔を通して外部を撮影するようにしたので、借家住まいのように扉または通路自体の改造が難しい場合にも、このような容器を適所に取り付けることで、泥棒等の無断侵入や盗難あるいは不正行為の発生を有効に防止することができる。

【０１７５】また請求項１２記載の発明によれば、郵便受けやドアホン等のように人の出入りする扉または通路の周辺に配置された防犯以外の所定の用途に使用される容器に孔を穿ち、撮像手段でこの孔を通して外部を撮影するようにしたので、借家住まいのように扉または通路自体の改造が難しい場合にも、このような容器を適所に取り付けることで、泥棒等の無断侵入や盗難あるいは不正行為の発生を有効に防止することができる。しかも撮像データ発信手段が、トリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信するようになっている。したがって、その容器自体を破壊されたり持ち去られるような場合でも、その行為を行った者の画像を取得することができ、結果的にそのような行為自体も防止することができる。

【０１７６】更に請求項１３および請求項１４記載の発明によれば、所定のタイミングを検出して撮像を行うことにしたので、撮像されたデータが有効なものが多く、かつ画像データの記憶容量が少なくて良いという利点がある。

【０１７７】また、請求項１５記載の発明によれば、トリガ手段は、予め定めた時間ごとに撮像手段を作動させるので、トリガ用に特別のセンサが不要である。また、人の検出を行う必要がないので、撮影の間隔が適正であれば確実に無断侵入や盗難あるいは不正行為に関する画像を記録することができるという長所がある。

【０１７８】更に請求項１６記載の発明によれば、撮像手段の近傍に外部の音を収集するマイクロフォンが配置されているので、採取するデータが豊富化する。

【０１７９】また請求項１７記載の発明によれば、孔はキーホールに似せた撮像のための孔であるので、ドア等の外観を損ねる可能性が少ない。

【０１８０】更に請求項１８記載の発明では、撮像の時刻情報が撮像データに組み込まれるので、泥棒等の無断侵入や盗難あるいは不正行為の起きた日時を推測できるだけでなく、たとえば子供が学校から帰ってきた時間等も簡単に知ることができる。

【０１８１】また請求項１９記載の発明によれば、記憶手段に静止画の画像データを１枚ずつ記憶する場合には、ある程度のメモリ容量に対して古い画像から順に上書きして記憶することで、メモリ不足を解消することができ、特別の事件が起きた時点で画像データを確実に再現することができる。

【０１８２】更に請求項２０記載の発明によれば、携帯端末を受信先とすることで迅速な対応が可能になる。また撮像側に音声の入出力装置を備えることで、訪問者との会話も可能になる。

【０１８３】また請求項２１記載の発明によれば、所定の受信先が駐輪場あるいは駐車場等に設けられた集中管理用の通信端末なので、それぞれの発信元ごとにデータが管理されれば、安価に盗難やいたずらの防止が可能になる。

【０１８４】更に請求項２２記載の発明によれば、撮像データを扉の配置されている側から所定の受信先に発信し、この通信中に受信先から開錠を指示する信号が送られてきたとき扉を開錠するので、扉の前の被写体を撮像データで確認したり音声による確認が可能であり、開錠の適否を的確に判別することができる。しかも、第三者の発呼によって開錠するのと異なるので、セキュリティを高度に保持することができる。

【０１８５】また請求項２３記載の発明によれば、撮像データ発信手段の受信先に撮像データを発信できないとき、予め定めた宛先にこれを転送し、その転送先がこれによる通信を行っている場合に限って遠隔操作による開錠を可能にしたので、本来の受信先の都合によって扉を開けるまでの待ち時間が長くなったり不可能となるといった事態が発生しない。また、本発明の場合にも扉の前の被写体を撮像データで確認したり音声による確認が可能であり、開錠の適否を的確に判別することができる。しかも、第三者の発呼によって開錠するのと異なるので、セキュリティを高度に保持することができる。

【０１８６】更に請求項２４記載の発明によれば、孔から撮像手段が撮像する障害となる明るさの変化を検出する障害検出手段と、この障害検出手段の検出が行われたとき警報音を出力する警報音出力手段を具備しているので、犯罪の予備行為が行われていることを第三者に知らせ、犯罪の発生を防止することができる。

【０１８７】また請求項２５記載の発明によれば、孔から撮像手段が撮像する障害となる明るさの変化を検出する障害検出手段と、この障害検出手段の検出が行われたとき警報を示すデータを所定の宛先に送出する警報データ送出手段を具備しているので、犯罪の予備行為が行われていることを関係者に知らせ、必要な措置を採らせることができる。

【０１８８】更に請求項２６記載の発明では、撮影を行うための孔を複数配置し、障害検出手段が１つの孔の障害を検出したとき他の孔の内部に配置された撮像手段を作動させることにしたので、撮影の妨害を行う者が１つの孔を塞ぐ等の行為を行っても、他の孔を通じて画像を取得することができ、セキュリティを向上させることができる。

【０１８９】また請求項２７または請求項２８記載の発明によれば、交通機関を走行させる者の多くが自己の通信のための携帯電話機等の通信端末を所持している事実に鑑みて、動力源始動検出手段が何らかの操作で動力源の始動を検出したときその周囲にその者の通信端末（特定通信端末）が存在していないときにはその特定通信端末に無線で通知することで、第三者による交通機関の無断走行等に対処することができる。

【０１９０】特に請求項２８記載の発明では、自動車の運転者がキーをキー挿入口に差したままにしているような場合であっても、これによる盗難事件を早期に解決することができる。また、特定通信端末とその交通機関との間で音声等の通信を行うことも簡単に可能になる。

【０１９１】更に請求項２９記載の発明によれば、たとえばキー挿入口の近傍等の第三者が気づきにくい位置等に撮像手段を配置しておけば、これらの者が不正に運転を試みた場合にその者の画像を特定通信端末に送信することが可能になる。また、交通機関の所有者の家族がその交通機関を運転しようとしたような場合には、画像を見ることによって第三者が不正に操作しているものでないことを簡単に確認することができる。

【０１９２】また請求項３０記載の発明によれば、交通機関側制御手段は、通知手段の通知に基づいて前記した特定通信端末から交通機関の走行停止あるいはドアのロックを示す信号が送信されてきたときこれに応じてその交通機関の走行停止あるいはドアのロックを行うので、交通機関が行方をくらましたり不正に運転を行った者が運転席から逃げるような事態の発生を防止することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施例におけるセキュリティシステムの構成の概要を表わした正面図である。

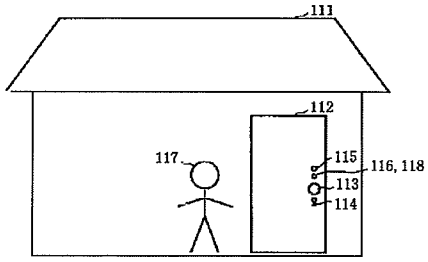
【図２】第１の実施例で使用されるセキュリティシステムの要部を示す断面図である。

【図３】第１の実施例の変形例としてのセキュリティシステムを屋内から見た要部斜視図である。

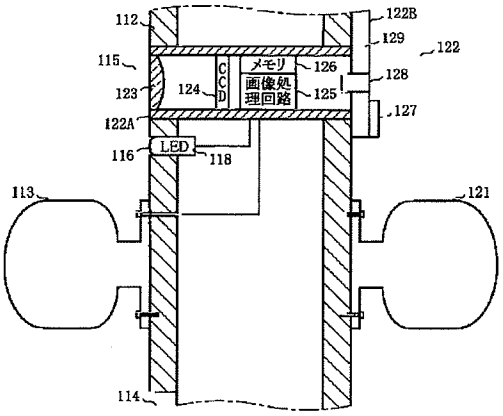
【図４】本発明の第２の実施例におけるセキュリティシステムの構成の概要を表わした正面図である。

【図５】第２の実施例における郵便ポストの構成を示した説明図である。
【図６】本発明の第３の実施例におけるセキュリティシステムが適用される金庫の斜視図である。
【図７】第３の実施例の第１の変形例として公衆トイレの防犯用のセキュリティシステムを表わした正面図である。
【図８】第３の実施例の第２の変形例としてエレベータの防犯用のセキュリティシステムを表わした正面図である。
【図９】本発明の第４の実施例におけるドアノブを使用したセキュリティシステムの要部を表わした平面図である。
【図１０】第４の実施例の変形例としてセキュリティシステムを使用した自動車の側面図である。
【図１１】本発明の第５の実施例のセキュリティシステムの概要を表わしたシステム構成図である。
【図１２】本発明の第６の実施例のセキュリティシステムの概要を表わしたもシステム構成図である。
【図１３】本発明の第７の実施例のセキュリティシステムの概要を表わした正面図である。
【図１４】本発明の第７の実施例におけるドアの要部の断面構造を表わした断面図である。
【図１５】本発明の第７の実施例における電子式錠装置の開錠制御の様子を表わした流れ図である。
【図１６】本発明の第７の実施例における悪意の来訪者が撮影を妨害する場合の対策としての処理の流れを表わした流れ図である。
【図１７】本発明の第８の実施例のセキュリティシステムの要部を表わした概略構成図である。
【図１８】第８の実施例の無線送受信器付制御装置の制御の概要を表わした流れ図である。
【図１９】本発明の第９の実施例のセキュリティシステムの概要を表わしたシステム構成図である。
【図２０】第９の実施例における装置内通信端末の制御の様子を表わした流れ図である。
【図２１】第９の実施例のセキュリティシステムの変形例としての特定携帯電話機のセキュリティシステムの要部を表わした説明図である。
【図２２】この変形例における装置内通信端末側の処理の流れを示した流れ図である。
【図２３】本発明の第１０の実施例のセキュリティシステムの要部を表わしたドアの正面図である。
【符号の説明】
１１１　家屋
１１２、２８２、２８３　ドア
１１３、２５３　ドアノブ
１１４　キーホール
１１８　赤外線ＬＥＤ（発光ダイオード）ランプ
１２２　画像ユニット
１２４　ＣＣＤ
１２６　メモリ
１２７　スイッチ
１２８、２６１　画像データ出力端子
１２９　液晶ディスプレイ
１４４、３０５、３２５　受信装置
１６１　郵便ポスト
１６６～１６８、１８３、１８４、２０６～２０９、２３２、２３３、２５８、２５９、５０４　孔
１７１、１８６　画像処理ユニット
１７３、１８５　送信アンテナ
１８１　金庫
１８２　扉
２０１　公衆トイレ
２３１　エレベータ
２５１、２５２　ノブ
２５７　画像撮影処理ユニット
２８１、３０２　自動車
２８４、２８５　ドアの把手
２８６、２８７　付属装置
３０１　自転車
３０３　バイク
３０４　駐車場
３２１、３２２　絵画
３２４　撮像送信ユニット
４０１　電子式錠装置
４０２　セキュリティ装置
４１１、４１３　基地局
４１４　セキュリティ管理会社
４１５　携帯電話端末
４２１　スピーカ部
４２２　マイク部
４２３　制御部
４２５　無線アンテナ
５０１　ボード
５０２　キー挿入口
５０３　孔の集合体
５０５　撮像装置
５０６　スピーカ
５０７　マイクロフォン
５０８　エンジン始動検出回路
５１１、５１１Ａ　装置内通信端末
５１２、５１２Ａ　携帯電話機
５５１　近距離通信カード
５９２　撮像用孔

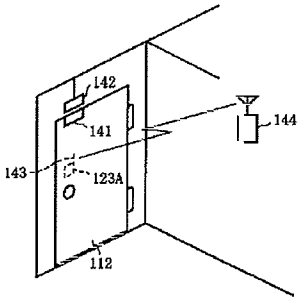
【図1】



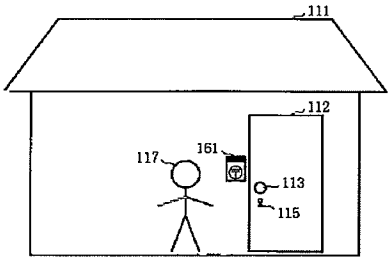
【図2】



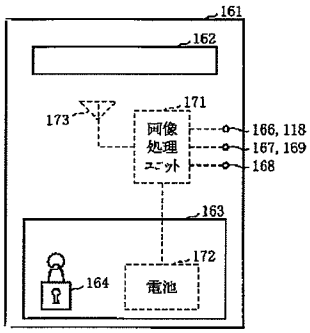
【図3】



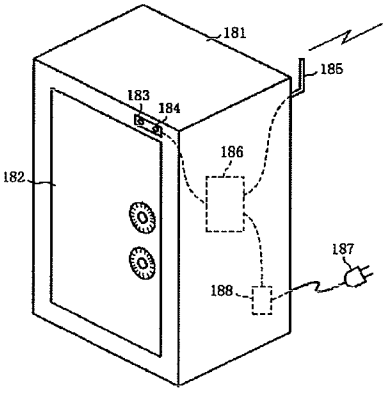
【図4】



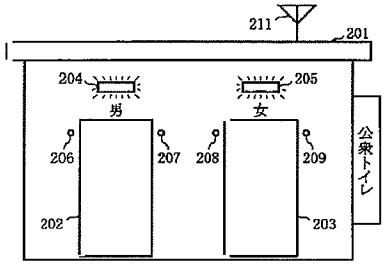
【図5】



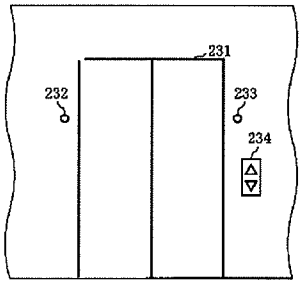
【図6】



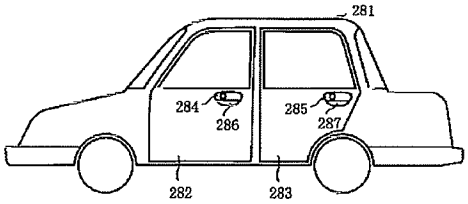
【図7】



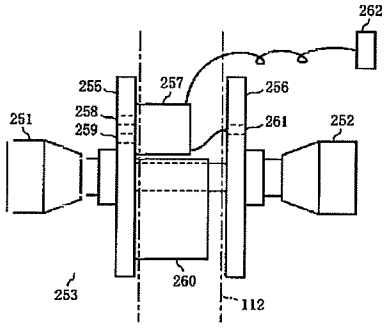
【図8】



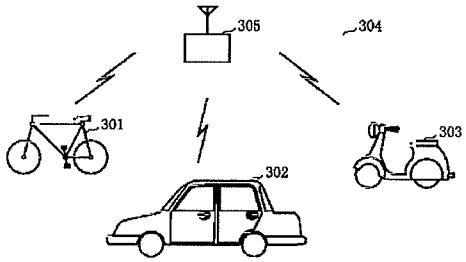
【図10】



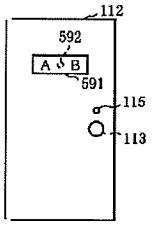
【図9】



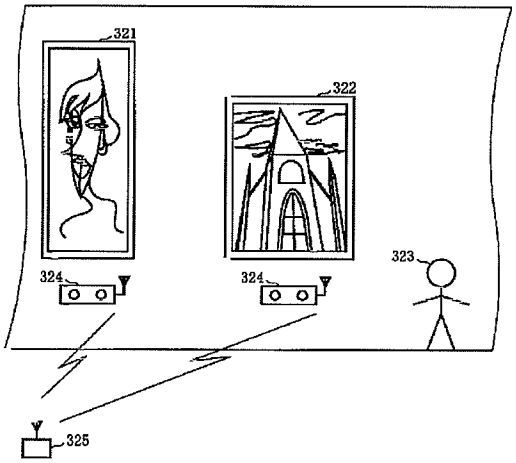
【図11】



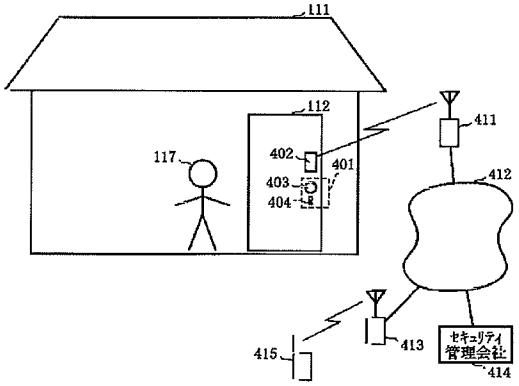
【図23】



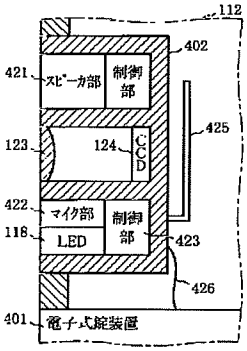
【図12】



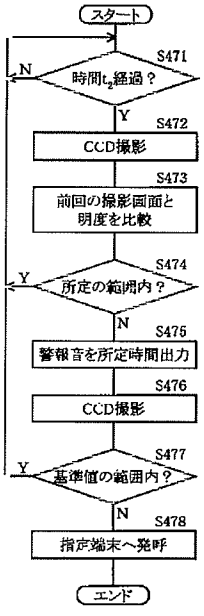
【図13】



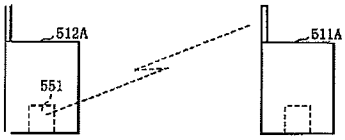
【図14】



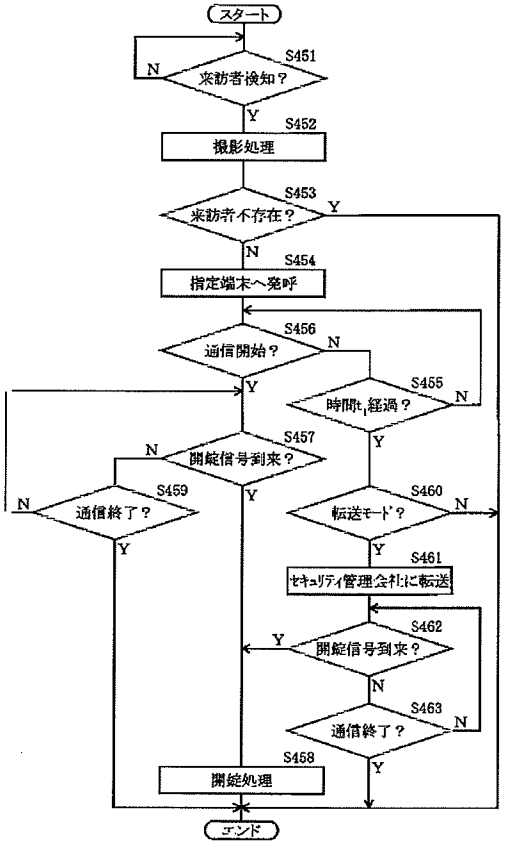
【図16】



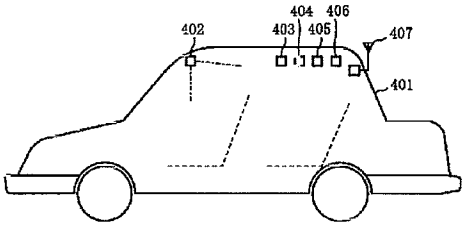
【図21】



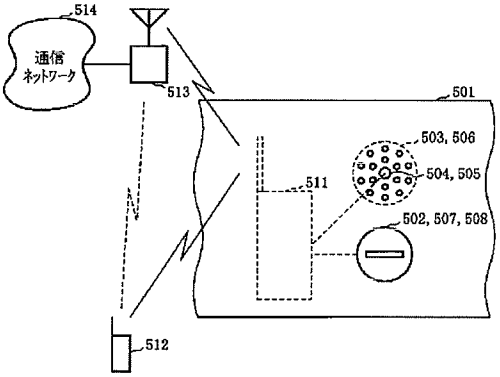
【図15】



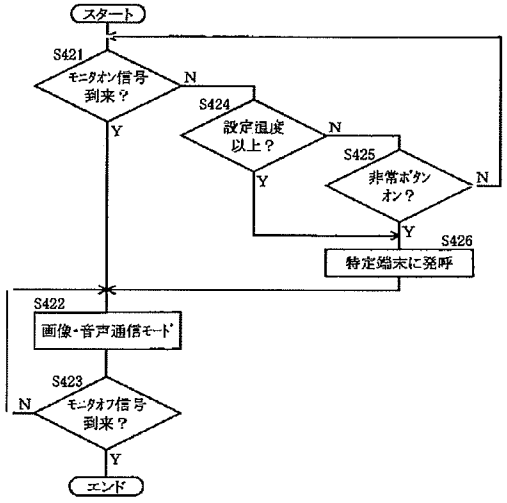
【図17】



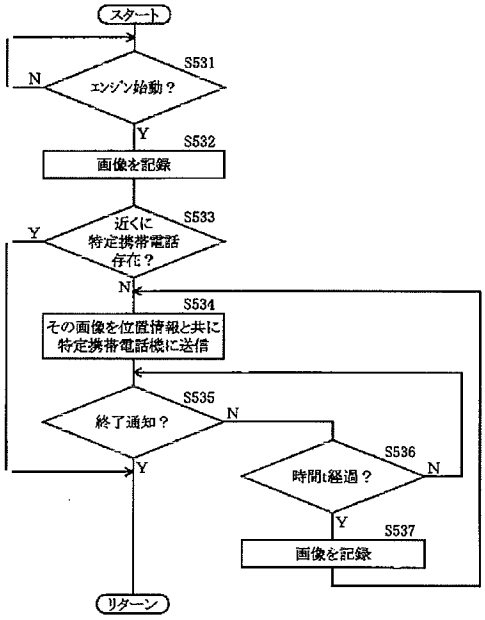
【図19】



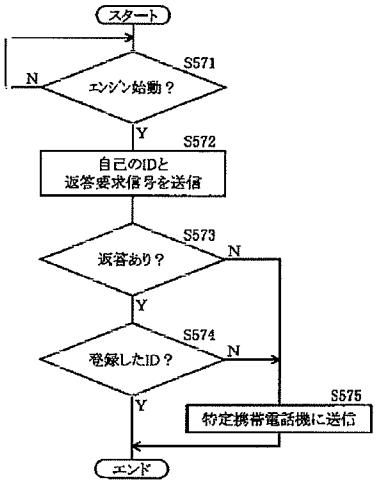
【図18】



【図20】



【図22】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		(参考)
G08B	21/00	G08B	21/00	E
H04N	5/225	H04N	5/225	C
	7/18		7/18	D
				H
// H04N	101:00		101:00	

(72)発明者 山口 寛一
東京都新宿区西新宿5－17－11

Fターム(参考) 2E250 AA21 BB08 BB15 BB65 CC00
CC21 CC28 DD06 FF24 FF25
FF27 FF36 HH00 HH01 JJ00
KK03 LL00 LL01 PP15 SS04
TT03
5C022 AA01 AA13 AC42
5C054 AA01 AA05 BA10 CC05 CE06
CH04 DA07 HA18
5C084 AA02 AA07 BB31 CC02 CC19
DD11
5C086 AA27 BA02 BA21 CA28 CB36
DA08 DA33 FA02